FIG.1

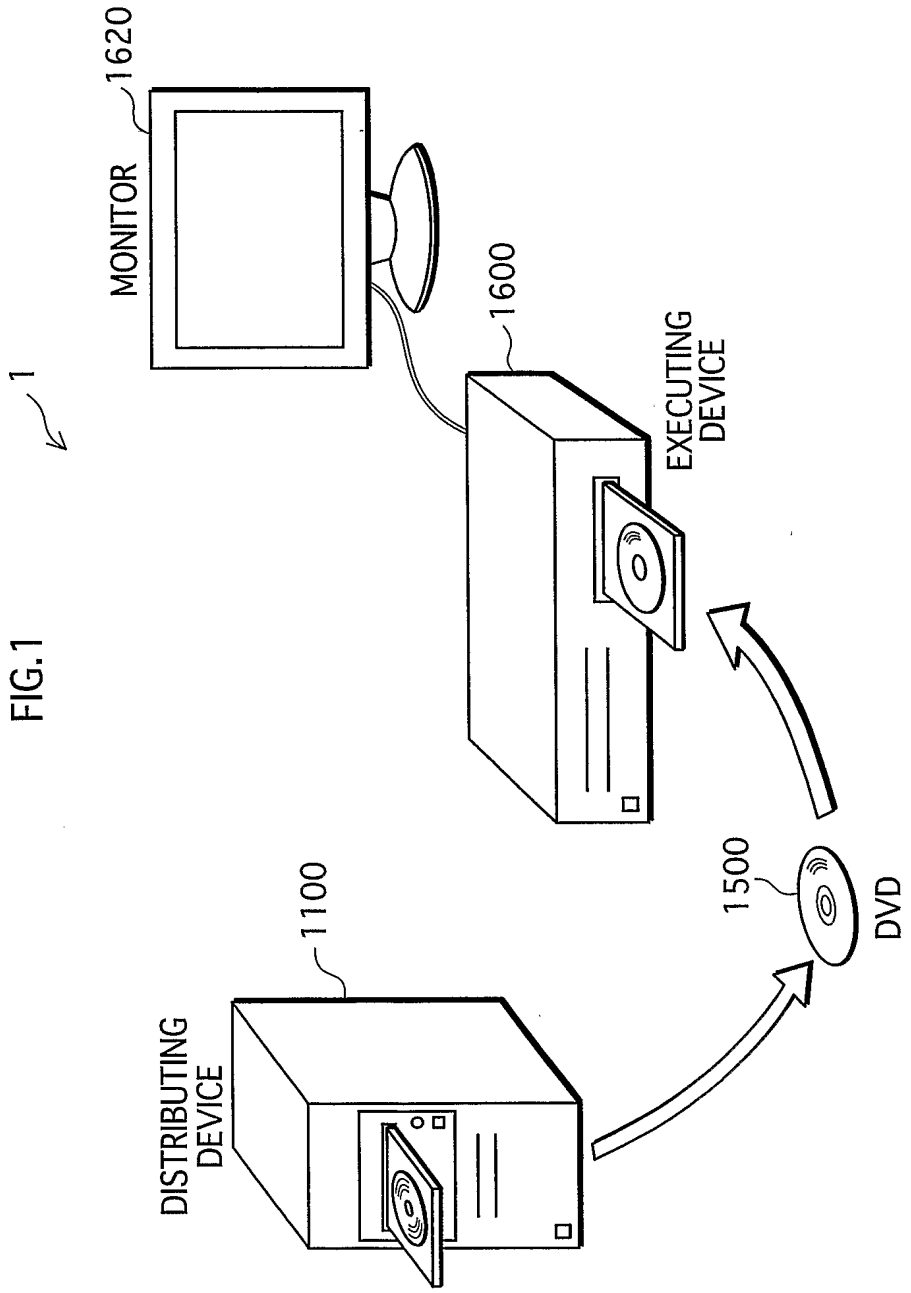

1
MONITOR
1620
1600
EXECUTING DEVICE
1500
DVD
1100
DISTRIBUTING DEVICE

FIG.2

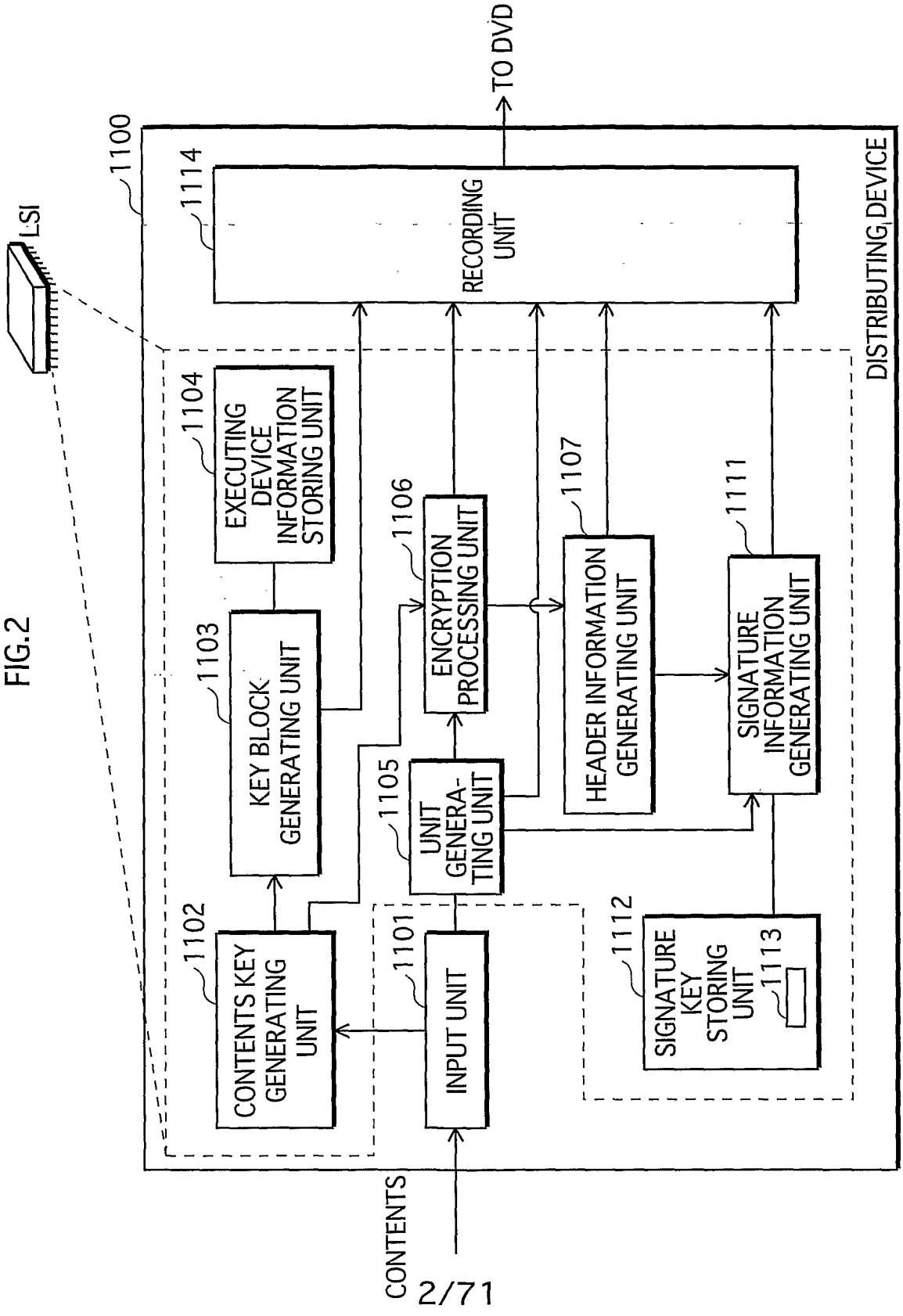

LSI
1100
DISTRIBUTING DEVICE
TO DVD
1114
RECORDING UNIT
1104
EXECUTING DEVICE INFORMATION STORING UNIT
1103
KEY BLOCK GENERATING UNIT
1106
ENCRYPTION PROCESSING UNIT
1107
HEADER INFORMATION GENERATING UNIT
1111
SIGNATURE INFORMATION GENERATING UNIT
1105
UNIT GENERA-TING UNIT
1102
CONTENTS KEY GENERATING UNIT
1101
INPUT UNIT
1112
SIGNATURE KEY STORING UNIT
1113
CONTENTS

FIG.3

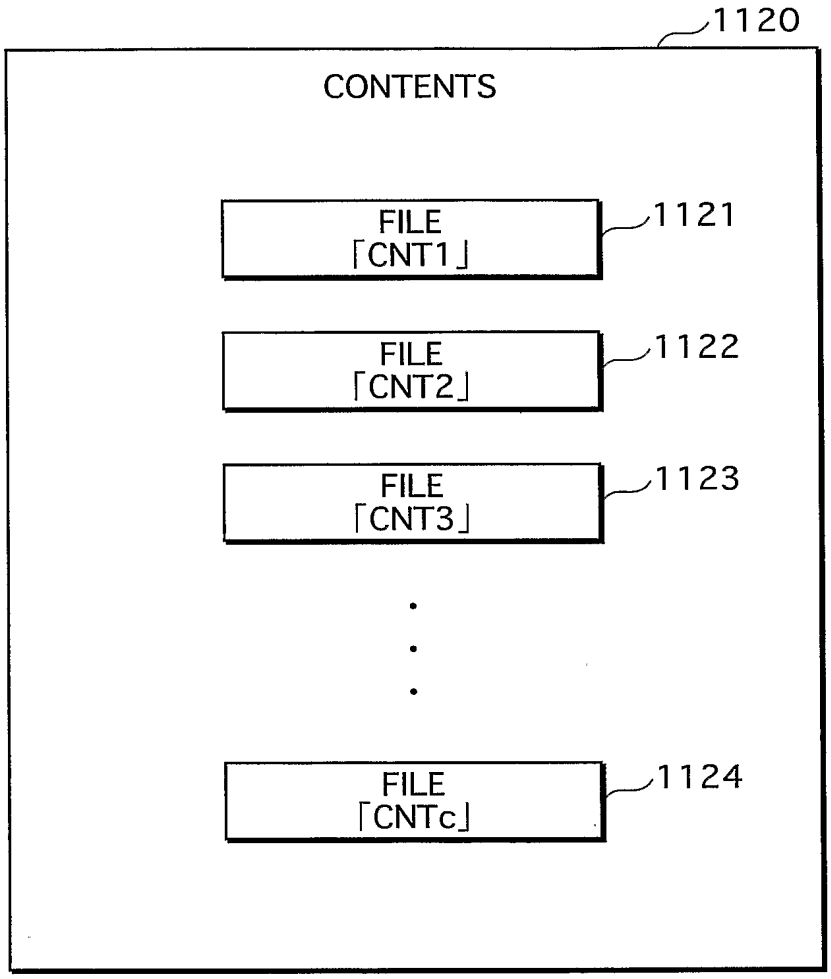

1120
CONTENTS
FILE
「CNT1」
1121
FILE
「CNT2」
1122
FILE
「CNT3」
1123
FILE
「CNTc」
1124

FIG.4

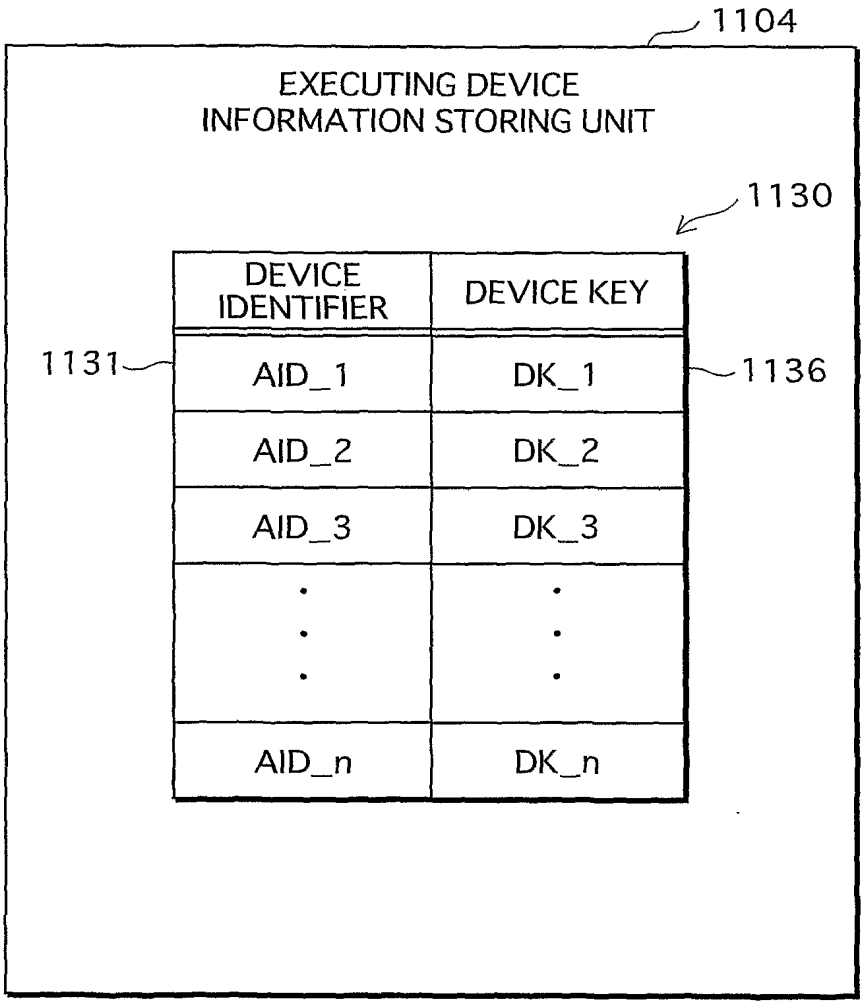

1104
EXECUTING DEVICE
INFORMATION STORING UNIT
1130
DEVICE IDENTIFIER
DEVICE KEY
1131
1136
AID_1
DK_1
AID_2
DK_2
AID_3
DK_3
AID_n
DK_n

FIG.5

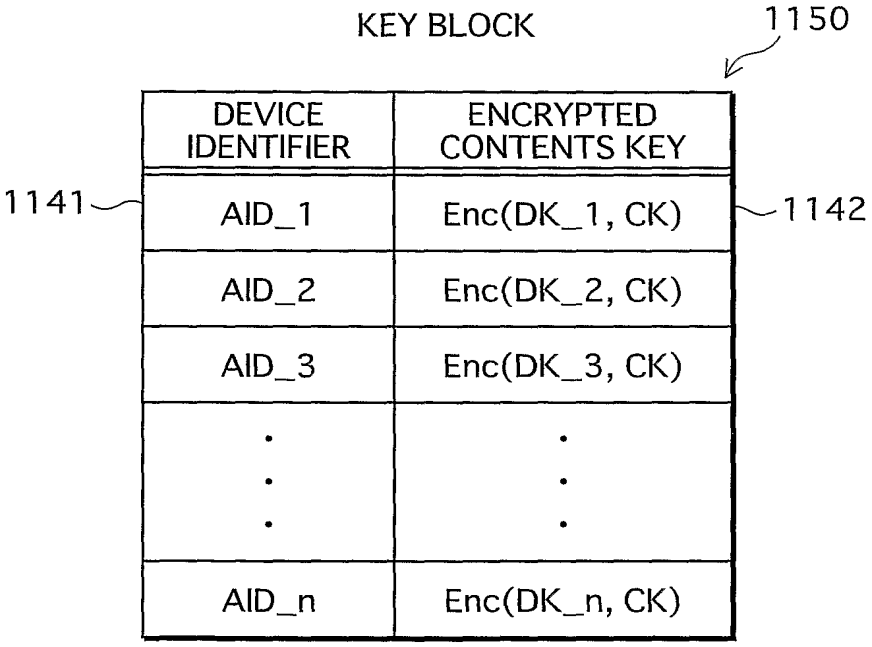

KEY BLOCK
1150
DEVICE IDENTIFIER
ENCRYPTED CONTENTS KEY
1141
1142
AID_1
Enc(DK_1, CK)
AID_2
Enc(DK_2, CK)
AID_3
Enc(DK_3, CK)
AID_n
Enc(DK_n, CK)

FIG.6

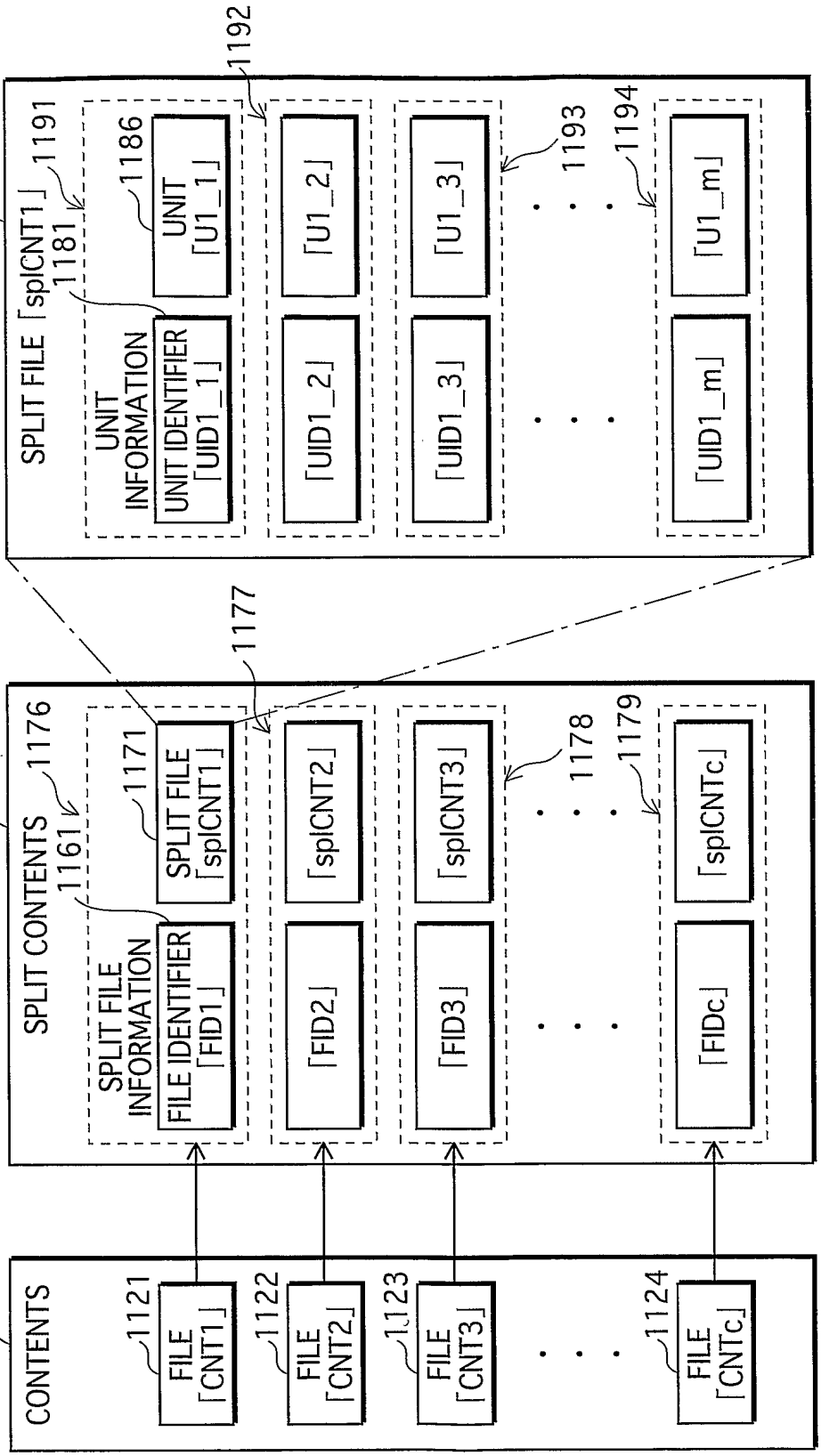

1120
CONTENTS
1121
FILE 「CNT1」
1122
FILE 「CNT2」
1123
FILE 「CNT3」
1124
FILE 「CNTc」
1160
SPLIT CONTENTS
1161
SPLIT FILE INFORMATION
FILE IDENTIFIER 「FID1」
「FID2」
「FID3」
「FIDc」
1171
SPLIT FILE 「splCNT1」
「splCNT2」
「splCNT3」
「splCNTc」
1176
1177
1178
1179
1171
SPLIT FILE 「splCNT1」
1181
UNIT INFORMATION
UNIT IDENTIFIER 「UID1_1」
「UID1_2」
「UID1_3」
「UID1_m」
1186
UNIT 「U1_1」
「U1_2」
「U1_3」
「U1_m」
1191
1192
1193
1194

FIG.7

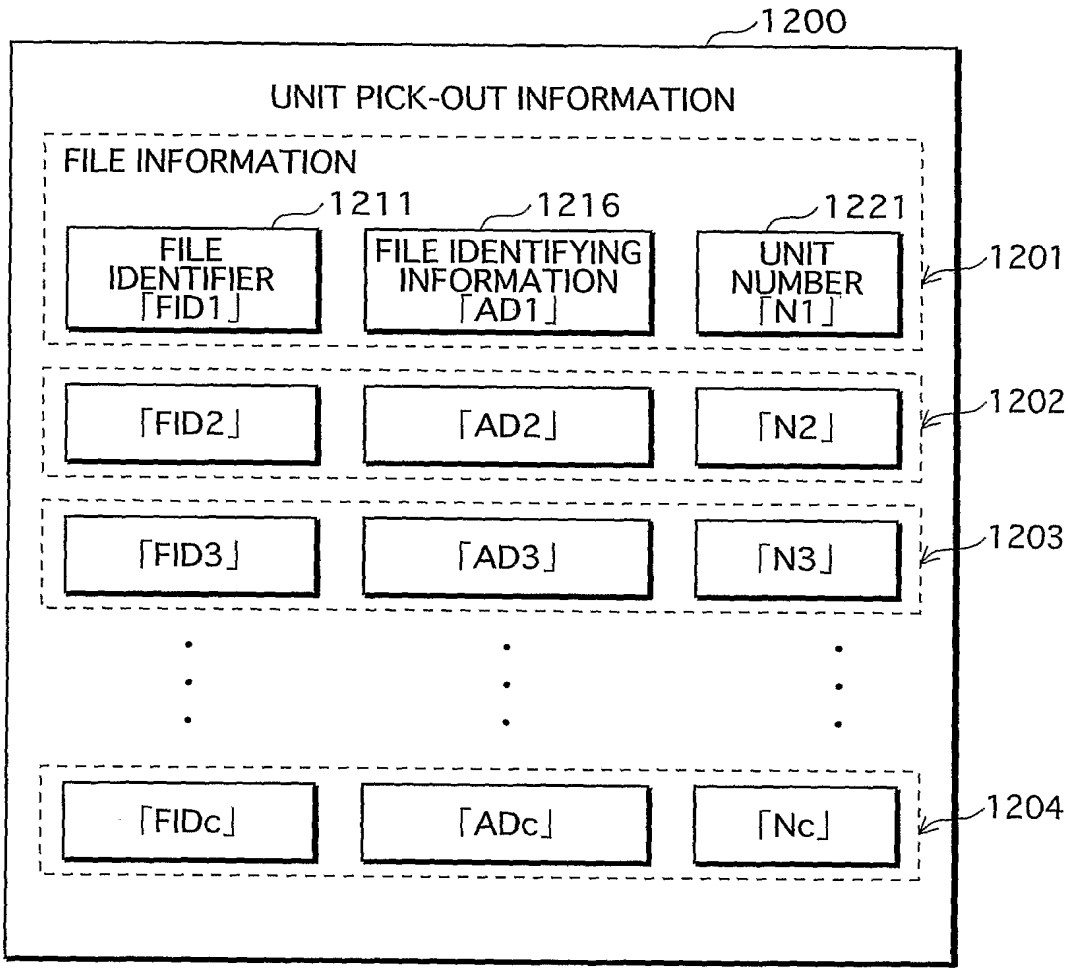

1200
UNIT PICK-OUT INFORMATION
FILE INFORMATION
1211
1216
1221
FILE IDENTIFIER 「FID1」
FILE IDENTIFYING INFORMATION 「AD1」
UNIT NUMBER 「N1」
1201
「FID2」
「AD2」
「N2」
1202
「FID3」
「AD3」
「N3」
1203
「FIDc」
「ADc」
「Nc」
1204

FIG.8

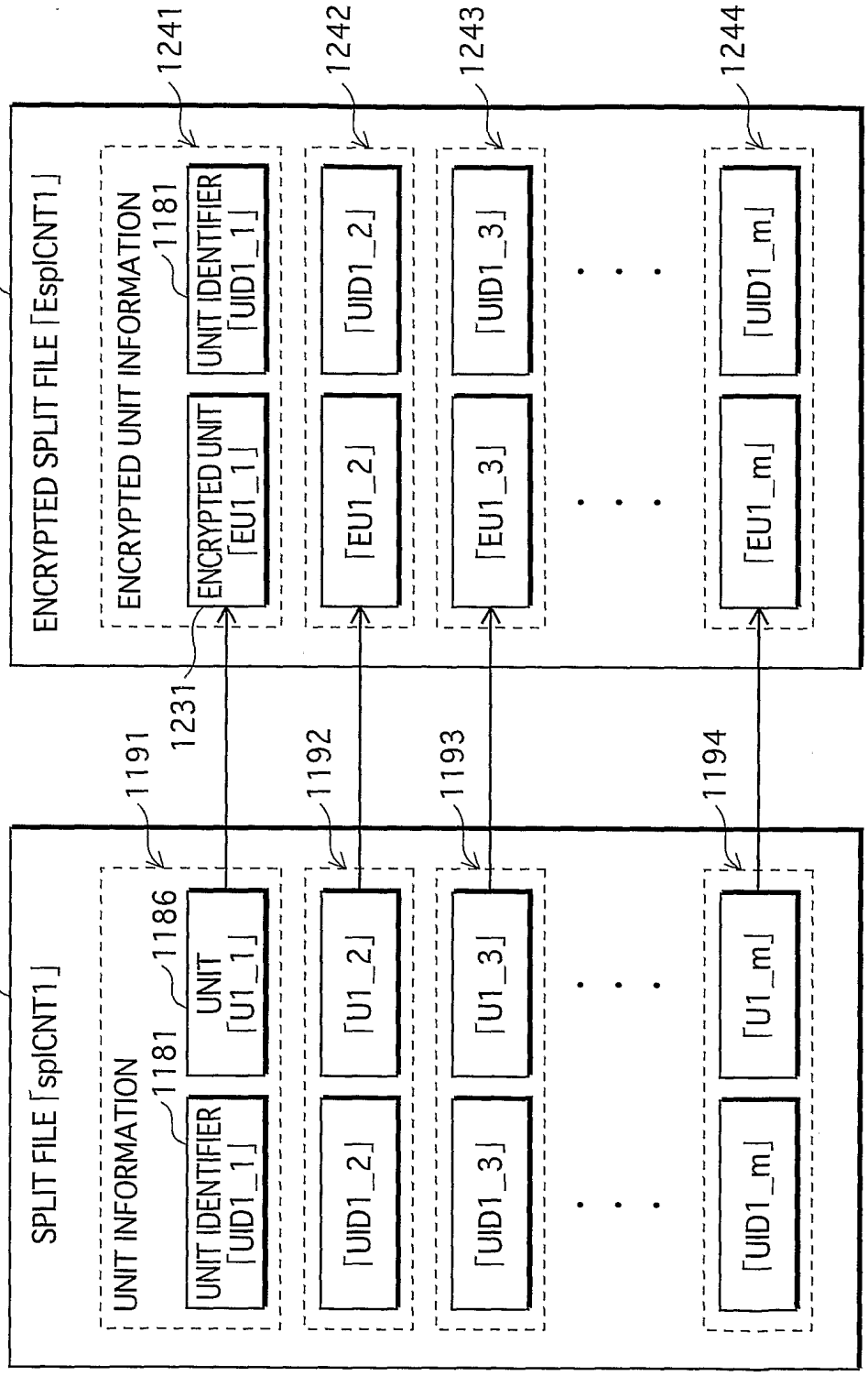

1251
ENCRYPTED SPLIT FILE 「EspICNT1」
1241
1242
1243
1244
ENCRYPTED UNIT INFORMATION
1181
UNIT IDENTIFIER 「UID1_1」
ENCRYPTED UNIT 「EU1_1」
「UID1_2」
「EU1_2」
「UID1_3」
「EU1_3」
「UID1_m」
「EU1_m」
1231
1191
1192
1193
1194
1171
SPLIT FILE 「spICNT1」
UNIT INFORMATION
1181
1186
UNIT 「U1_1」
「UID1_2」
「U1_2」
「UID1_3」
「U1_3」
「UID1_m」
「U1_m」

FIG.9

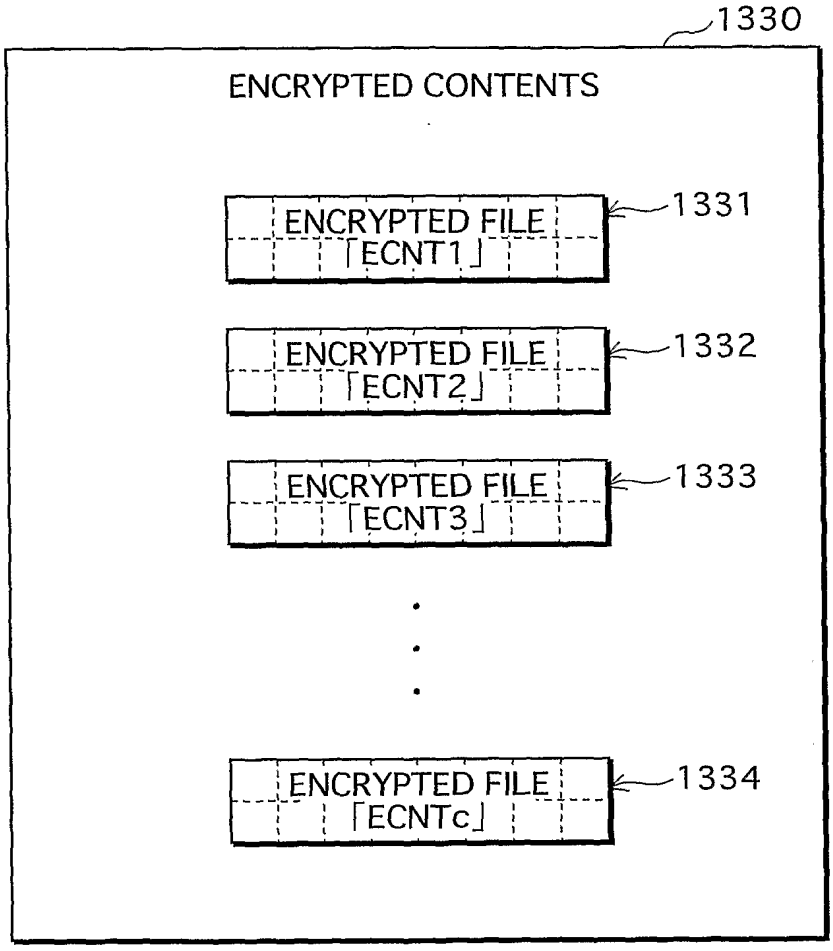

1330
ENCRYPTED CONTENTS
ENCRYPTED FILE
「ECNT1」
1331
ENCRYPTED FILE
「ECNT2」
1332
ENCRYPTED FILE
「ECNT3」
1333
ENCRYPTED FILE
「ECNTc」
1334

FIG.10

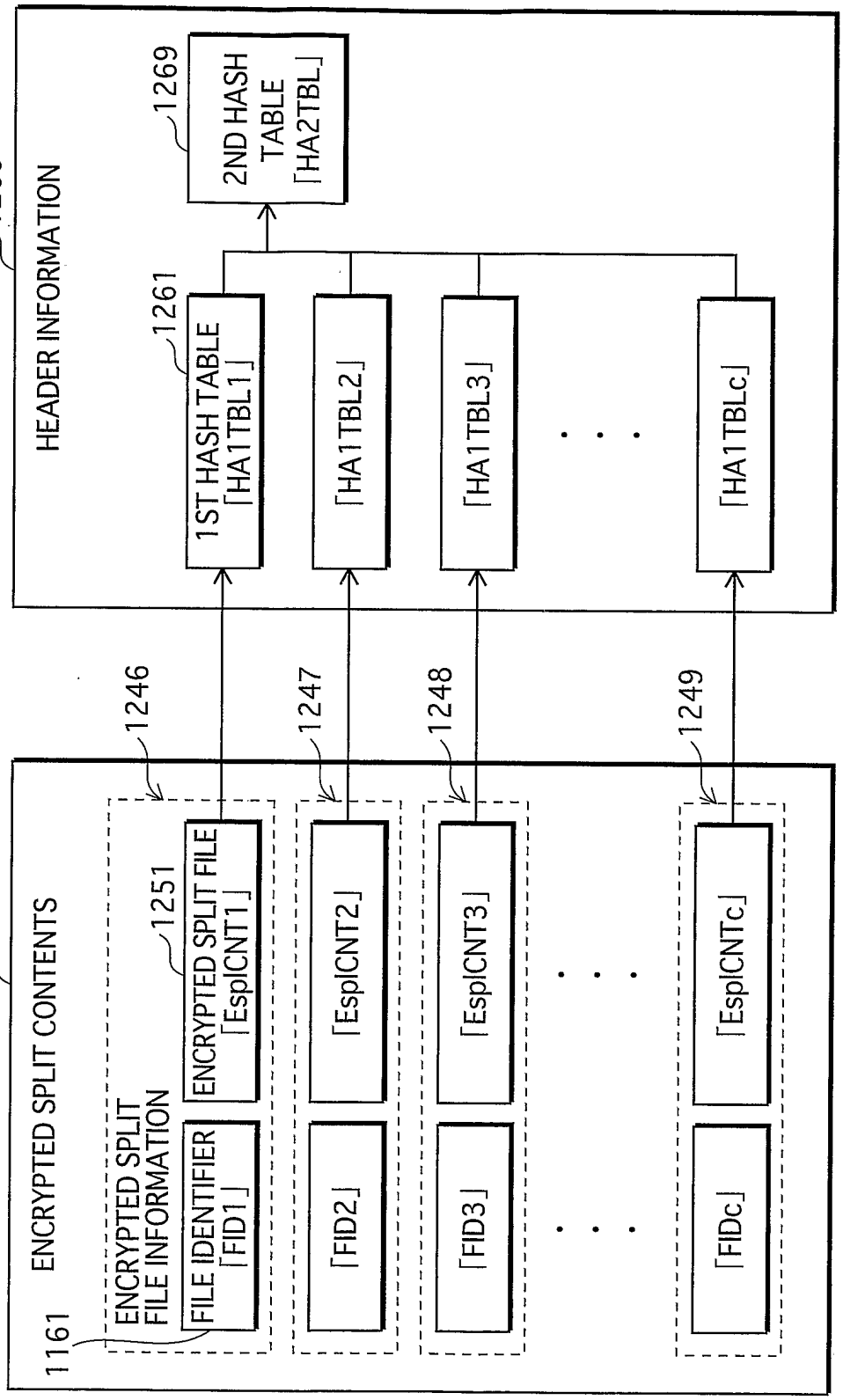

1260
HEADER INFORMATION
1269
2ND HASH TABLE 「HA2TBL」
1261
1ST HASH TABLE 「HA1TBL1」
「HA1TBL2」
「HA1TBL3」
「HA1TBLc」
1210
ENCRYPTED SPLIT CONTENTS
1246
1247
1248
1249
1251
ENCRYPTED SPLIT FILE 「EsplCNT1」
「EsplCNT2」
「EsplCNT3」
「EsplCNTc」
1161
ENCRYPTED SPLIT FILE INFORMATION
FILE IDENTIFIER 「FID1」
「FID2」
「FID3」
「FIDc」

FIG.11

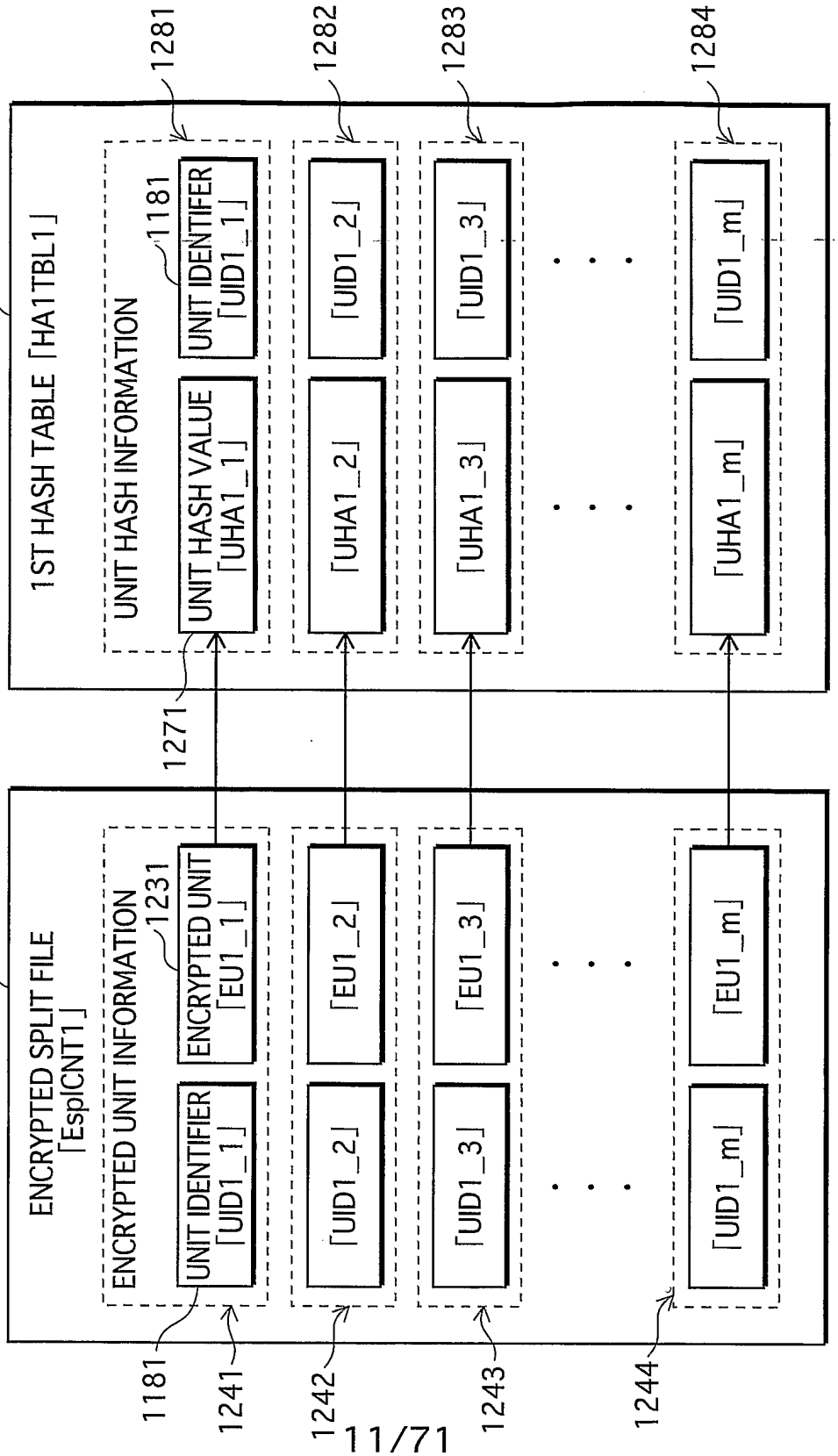

1261
1ST HASH TABLE 「HA1TBL1」
UNIT HASH INFORMATION
1181
UNIT IDENTIFER 「UID1_1」
UNIT HASH VALUE 「UHA1_1」
1281
1282
1283
1284
「UID1_2」
「UHA1_2」
「UID1_3」
「UHA1_3」
「UID1_m」
「UHA1_m」
1271
1251
ENCRYPTED SPLIT FILE 「EsplCNT1」
ENCRYPTED UNIT INFORMATION
1231
ENCRYPTED UNIT 「EU1_1」
UNIT IDENTIFIER 「UID1_1」
「EU1_2」
「UID1_2」
「EU1_3」
「UID1_3」
「EU1_m」
「UID1_m」
1181
1241
1242
1243
1244

FIG.12

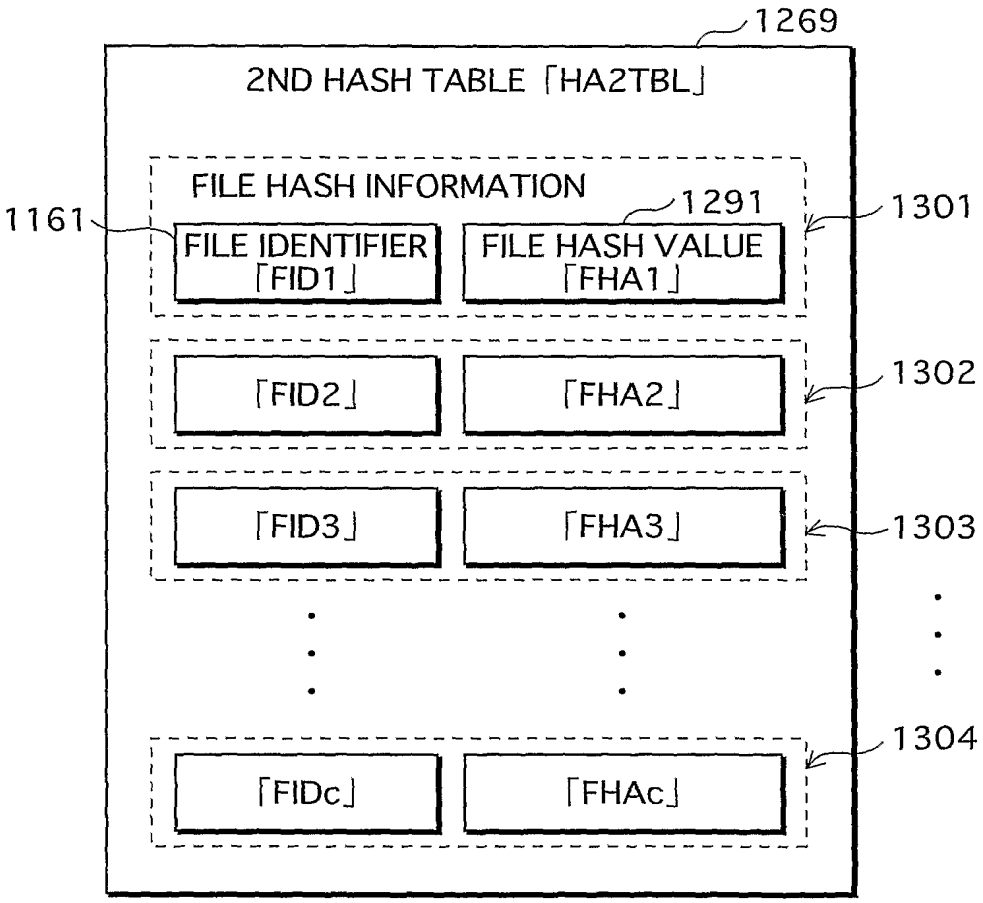

1269
2ND HASH TABLE「HA2TBL」
FILE HASH INFORMATION
1291
1161
1301
FILE IDENTIFIER 「FID1」
FILE HASH VALUE 「FHA1」
1302
「FID2」
「FHA2」
1303
「FID3」
「FHA3」
1304
「FIDc」
「FHAc」

FIG.13

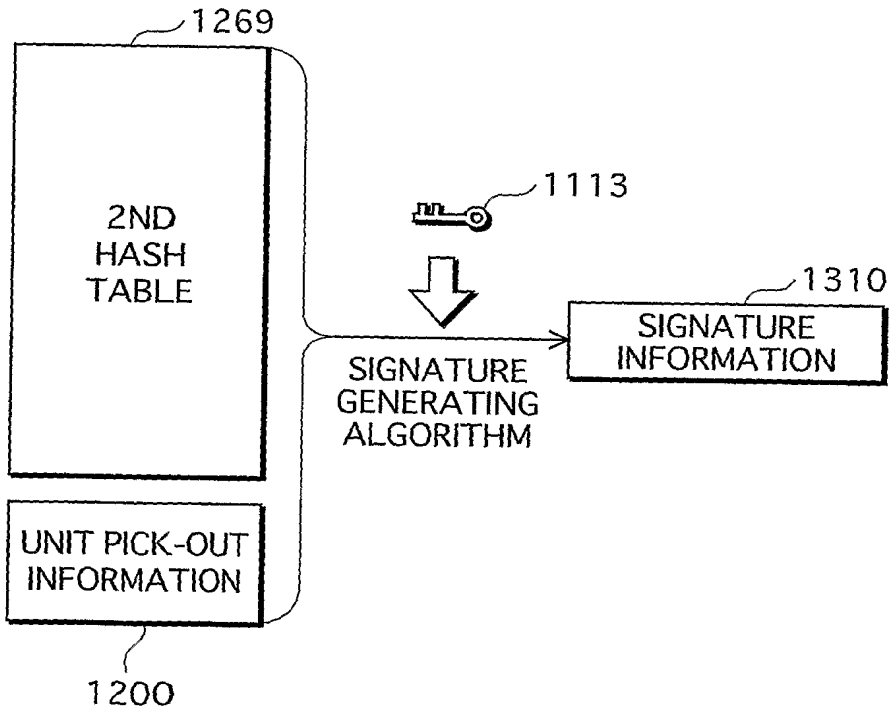

1269
2ND HASH TABLE
1113
1310
SIGNATURE INFORMATION
SIGNATURE GENERATING ALGORITHM
UNIT PICK-OUT INFORMATION
1200

FIG.14

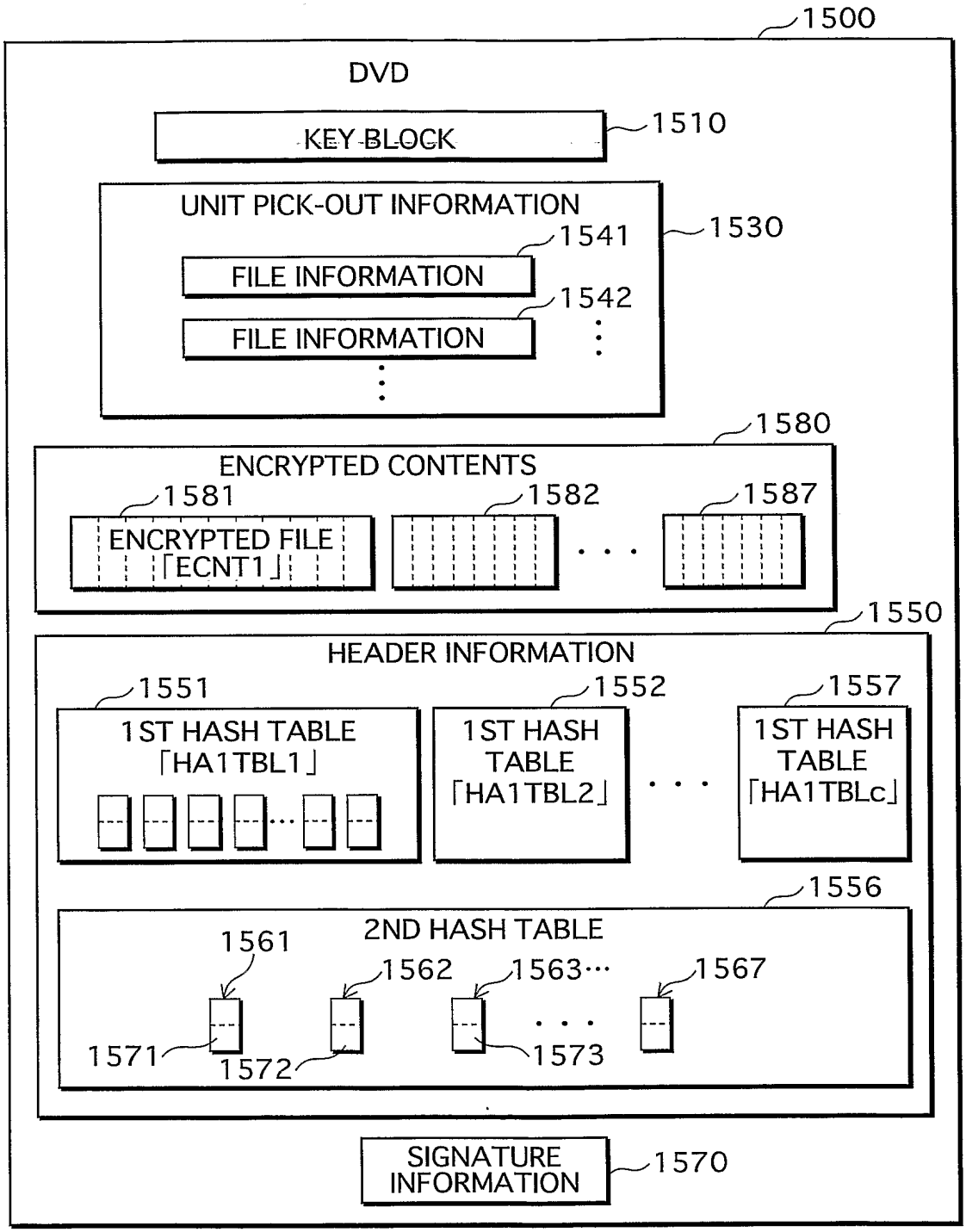

1500
DVD
KEY BLOCK
1510
UNIT PICK-OUT INFORMATION
1530
1541
FILE INFORMATION
1542
FILE INFORMATION
1580
ENCRYPTED CONTENTS
1581
1582
1587
ENCRYPTED FILE 「ECNT1」
1550
HEADER INFORMATION
1551
1552
1557
1ST HASH TABLE 「HA1TBL1」
1ST HASH TABLE 「HA1TBL2」
1ST HASH TABLE 「HA1TBLc」
1556
2ND HASH TABLE
1561
1562
1563
1567
1571
1572
1573
SIGNATURE INFORMATION
1570

FIG.15

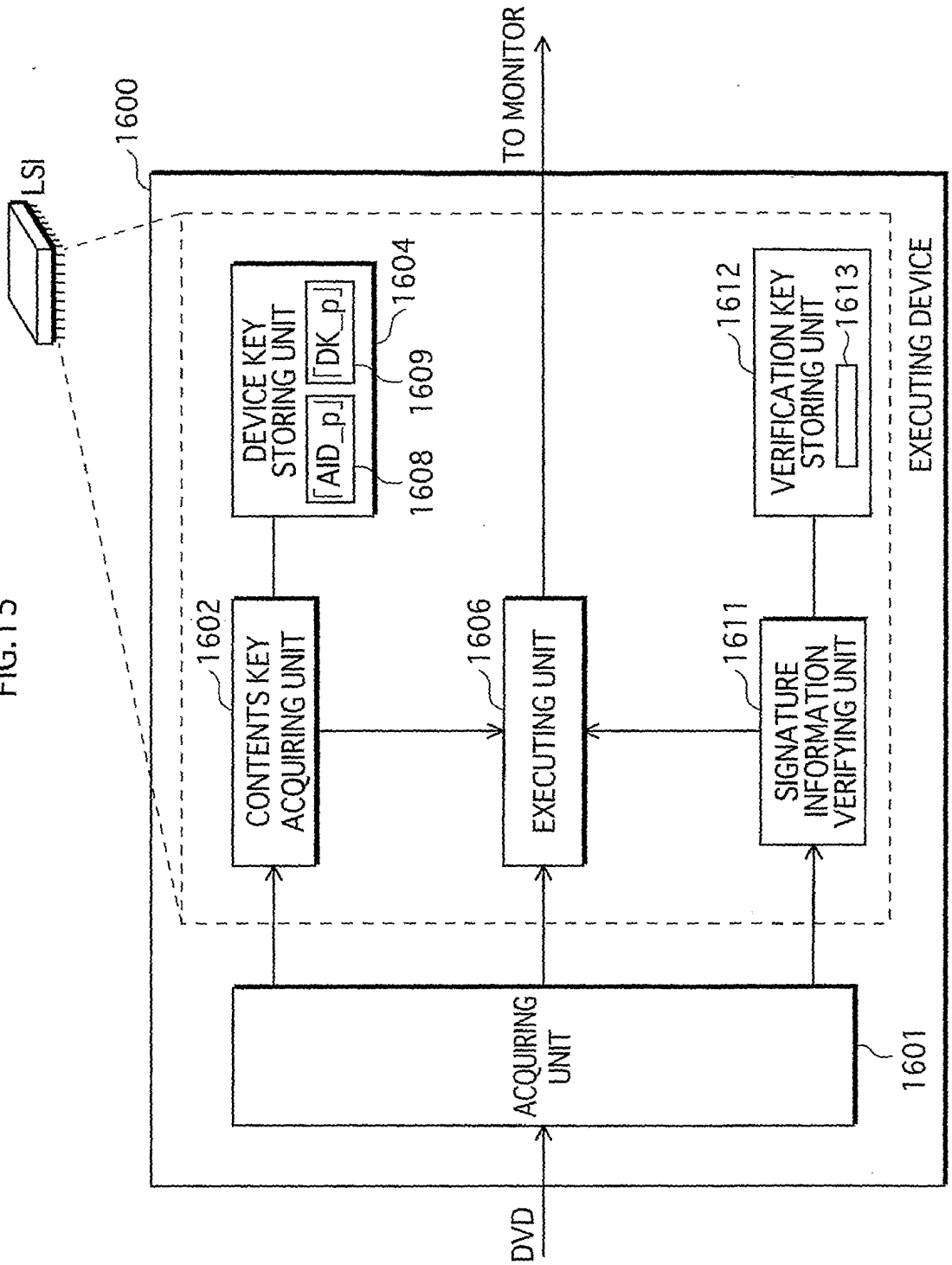

LSI
1600
TO MONITOR
DEVICE KEY STORING UNIT
[AID_p]
[DK_p]
1604
1609
1608
VERIFICATION KEY STORING UNIT
1612
1613
EXECUTING DEVICE
1602
CONTENTS KEY ACQUIRING UNIT
1606
EXECUTING UNIT
1611
SIGNATURE INFORMATION VERIFYING UNIT
ACQUIRING UNIT
1601
DVD

FIG.16

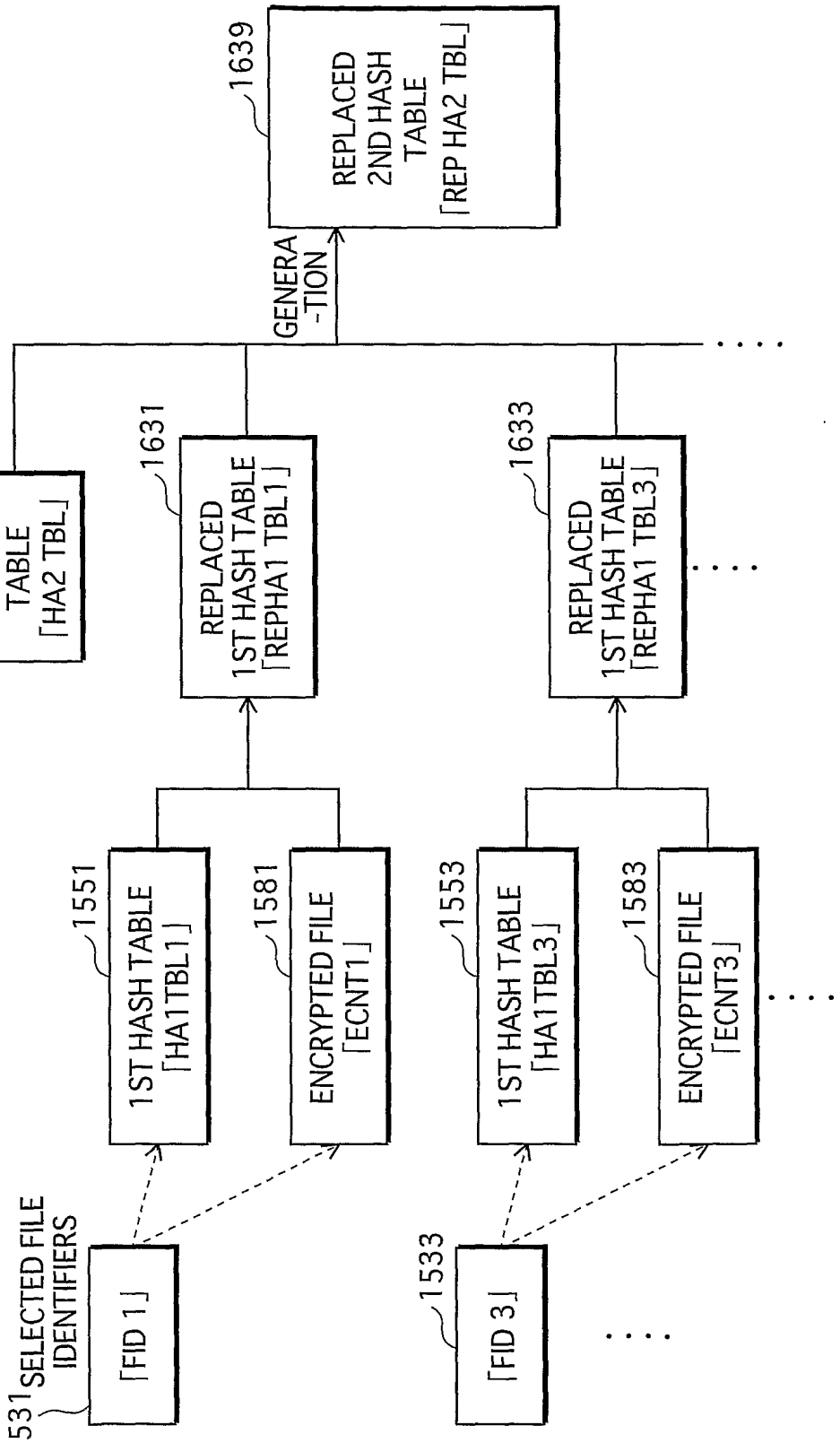

1639
REPLACED 2ND HASH TABLE 「REP HA2 TBL」
GENERA -TION
1556
2ND HASH TABLE 「HA2 TBL」
1631
REPLACED 1ST HASH TABLE 「REPHA1 TBL1」
1633
REPLACED 1ST HASH TABLE 「REPHA1 TBL3」
1551
1ST HASH TABLE 「HA1TBL1」
1581
ENCRYPTED FILE 「ECNT1」
1553
1ST HASH TABLE 「HA1TBL3」
1583
ENCRYPTED FILE 「ECNT3」
1531 SELECTED FILE IDENTIFIERS
「FID 1」
1533
「FID 3」

FIG.17

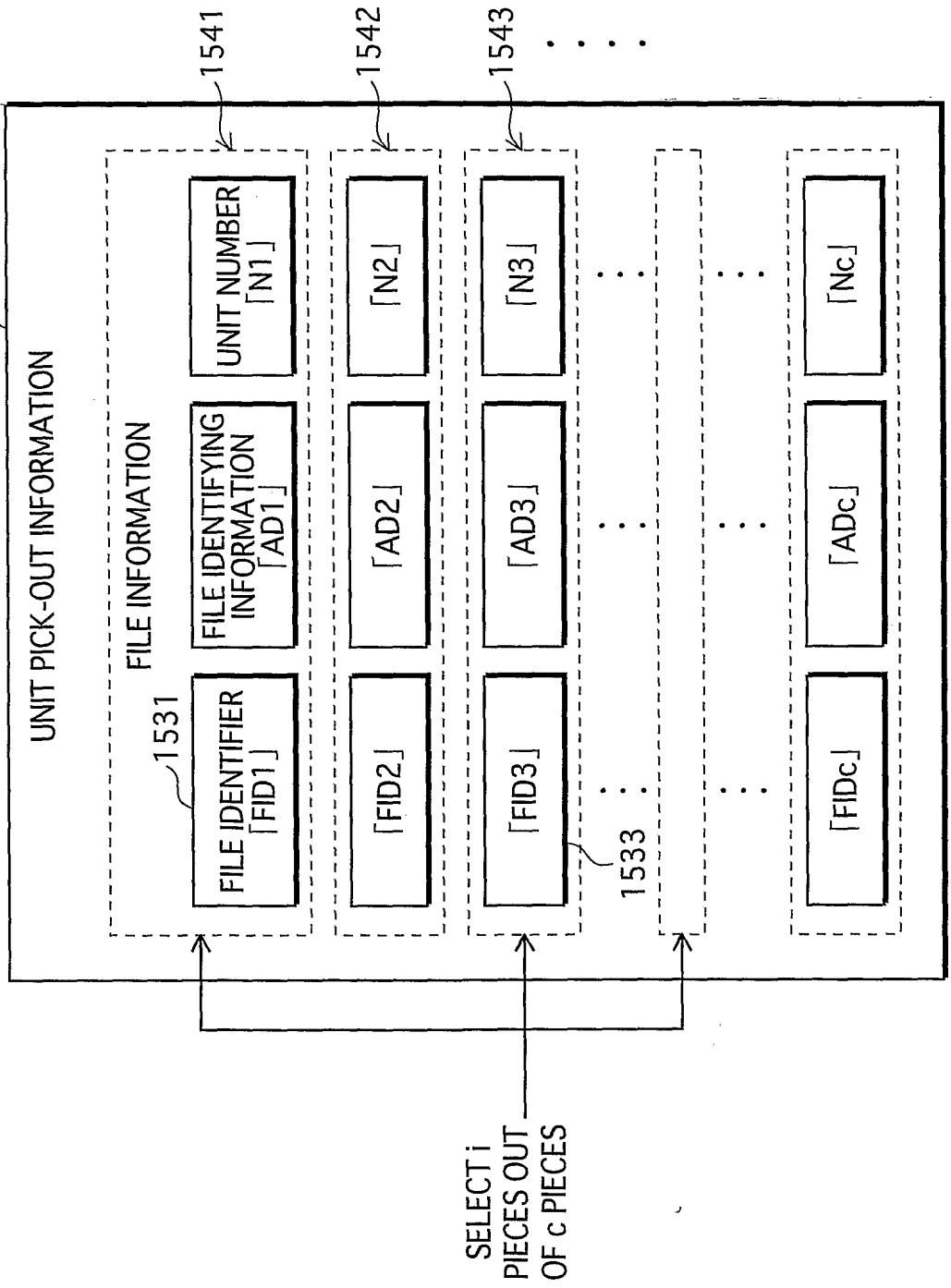

1530
UNIT PICK-OUT INFORMATION
1541
1542
1543
FILE INFORMATION
1531
FILE IDENTIFIER 「FID1」
FILE IDENTIFYING INFORMATION 「AD1」
UNIT NUMBER 「N1」
「FID2」
「AD2」
「N2」
「FID3」
「AD3」
「N3」
1533
「FIDc」
「ADc」
「Nc」
SELECT i PIECES OUT OF c PIECES

FIG.18

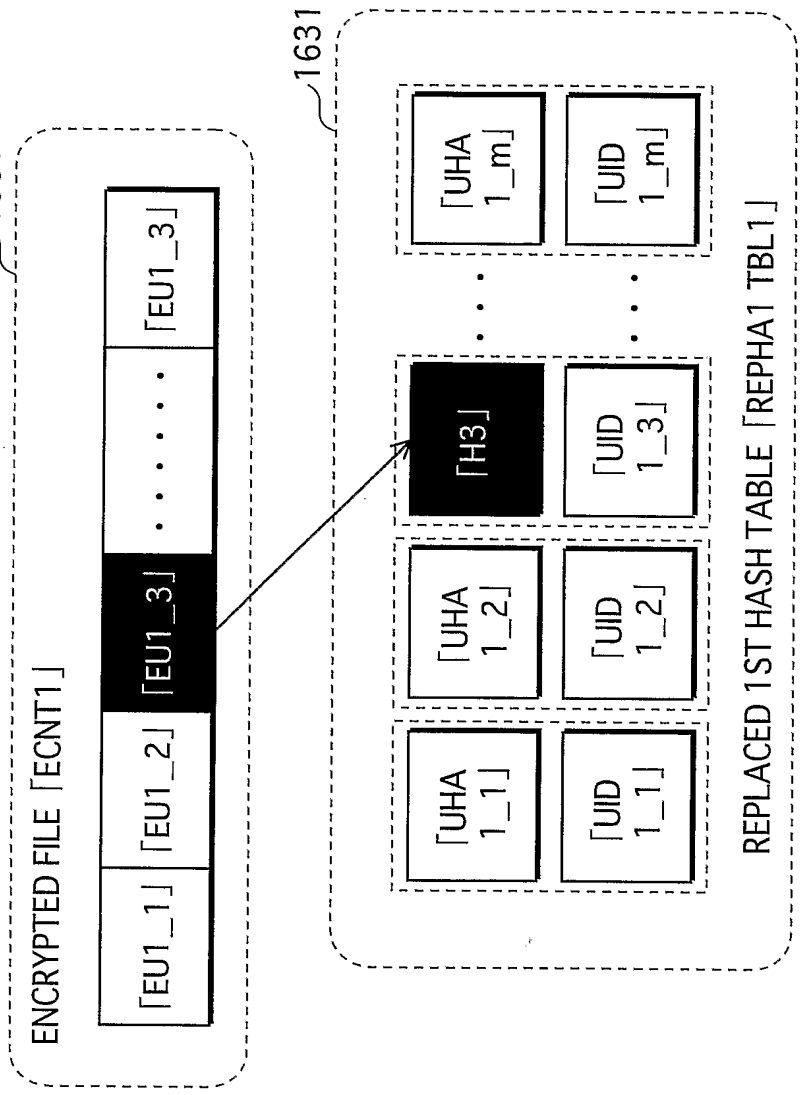

1581
ENCRYPTED FILE 「ECNT1」
「EU1_1」
「EU1_2」
「EU1_3」
「EU1_3」
1631
REPLACED 1ST HASH TABLE 「REPHA1 TBL1」
「UHA 1_1」
「UID 1_1」
「UHA 1_2」
「UID 1_2」
「H3」
「UID 1_3」
「UHA 1_m」
「UID 1_m」

FIG.19

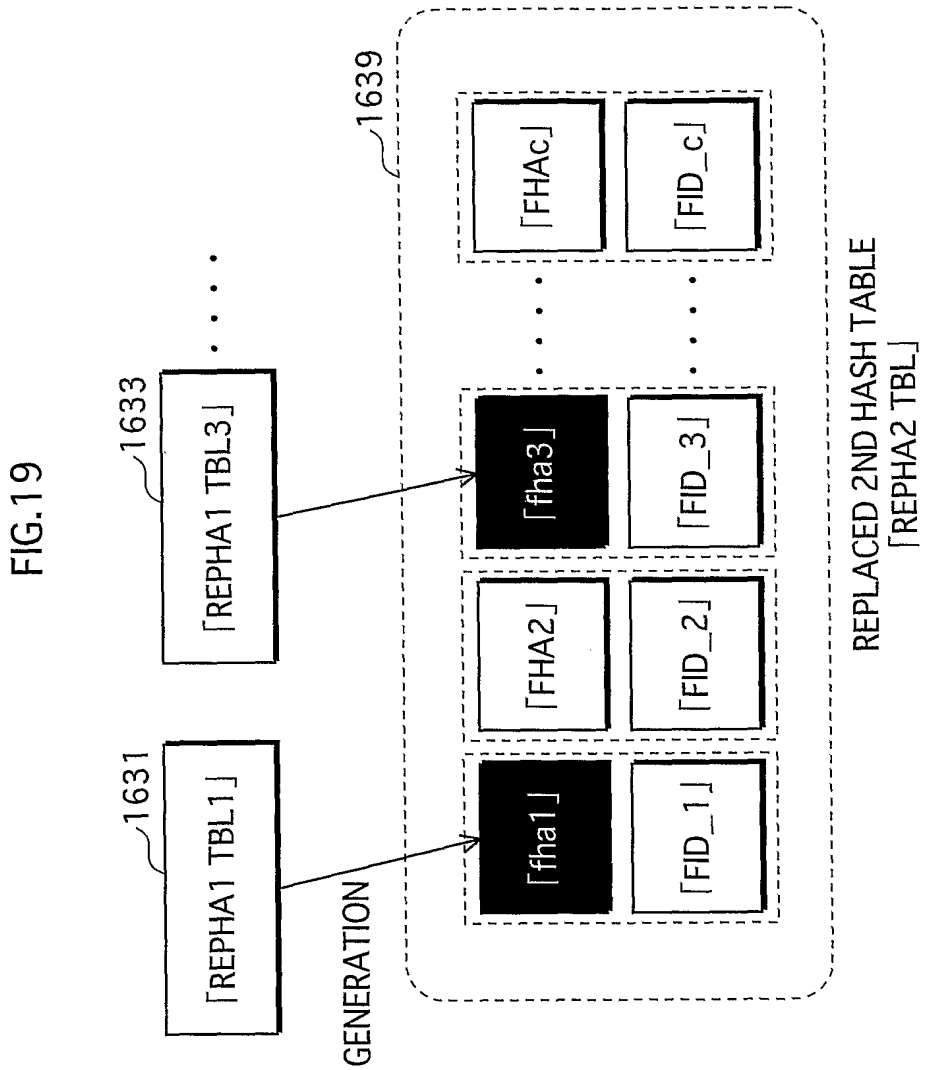

1639
「FHAc」
「FID_c」
1633
「REPHA1 TBL3」
「fha3」
「FID_3」
「FHA2」
「FID_2」
1631
「REPHA1 TBL1」
「fha1」
「FID_1」
GENERATION
REPLACED 2ND HASH TABLE
「REPHA2 TBL」

FIG.20

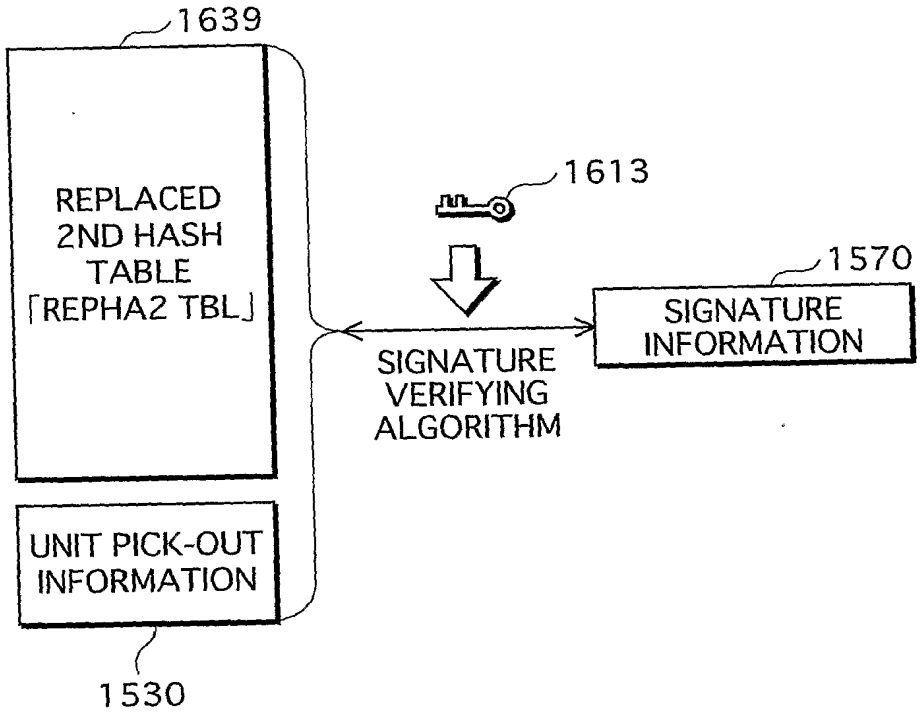

1639
REPLACED 2ND HASH TABLE [REPHA2 TBL]
UNIT PICK-OUT INFORMATION
1530
1613
SIGNATURE VERIFYING ALGORITHM
1570
SIGNATURE INFORMATION

FIG.21

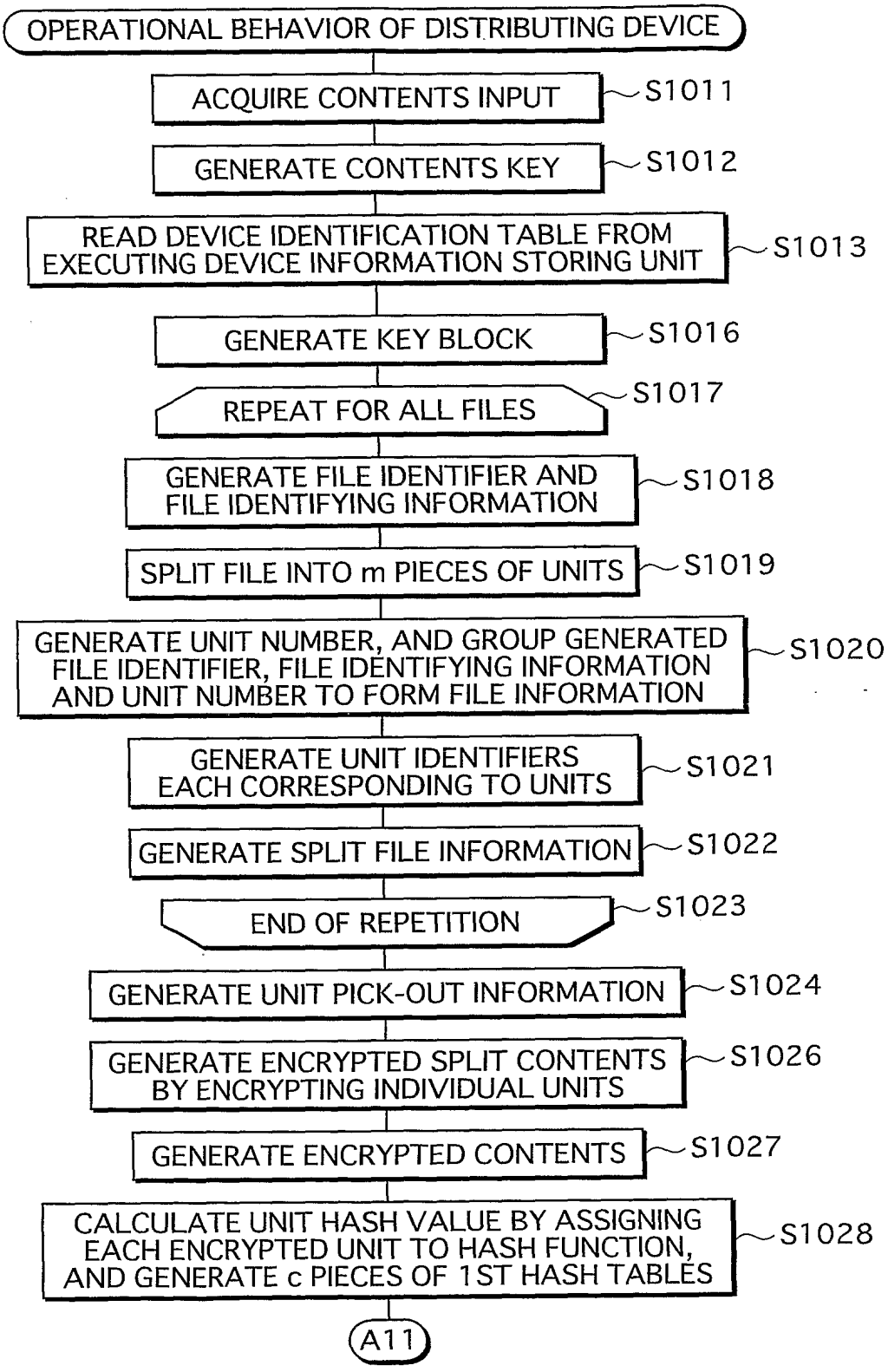

OPERATIONAL BEHAVIOR OF DISTRIBUTING DEVICE
ACQUIRE CONTENTS INPUT
S1011
GENERATE CONTENTS KEY
S1012
READ DEVICE IDENTIFICATION TABLE FROM EXECUTING DEVICE INFORMATION STORING UNIT
S1013
GENERATE KEY BLOCK
S1016
REPEAT FOR ALL FILES
S1017
GENERATE FILE IDENTIFIER AND FILE IDENTIFYING INFORMATION
S1018
SPLIT FILE INTO m PIECES OF UNITS
S1019
GENERATE UNIT NUMBER, AND GROUP GENERATED FILE IDENTIFIER, FILE IDENTIFYING INFORMATION AND UNIT NUMBER TO FORM FILE INFORMATION
S1020
GENERATE UNIT IDENTIFIERS EACH CORRESPONDING TO UNITS
S1021
GENERATE SPLIT FILE INFORMATION
S1022
END OF REPETITION
S1023
GENERATE UNIT PICK-OUT INFORMATION
S1024
GENERATE ENCRYPTED SPLIT CONTENTS BY ENCRYPTING INDIVIDUAL UNITS
S1026
GENERATE ENCRYPTED CONTENTS
S1027
CALCULATE UNIT HASH VALUE BY ASSIGNING EACH ENCRYPTED UNIT TO HASH FUNCTION, AND GENERATE c PIECES OF 1ST HASH TABLES
S1028
A11

FIG.22

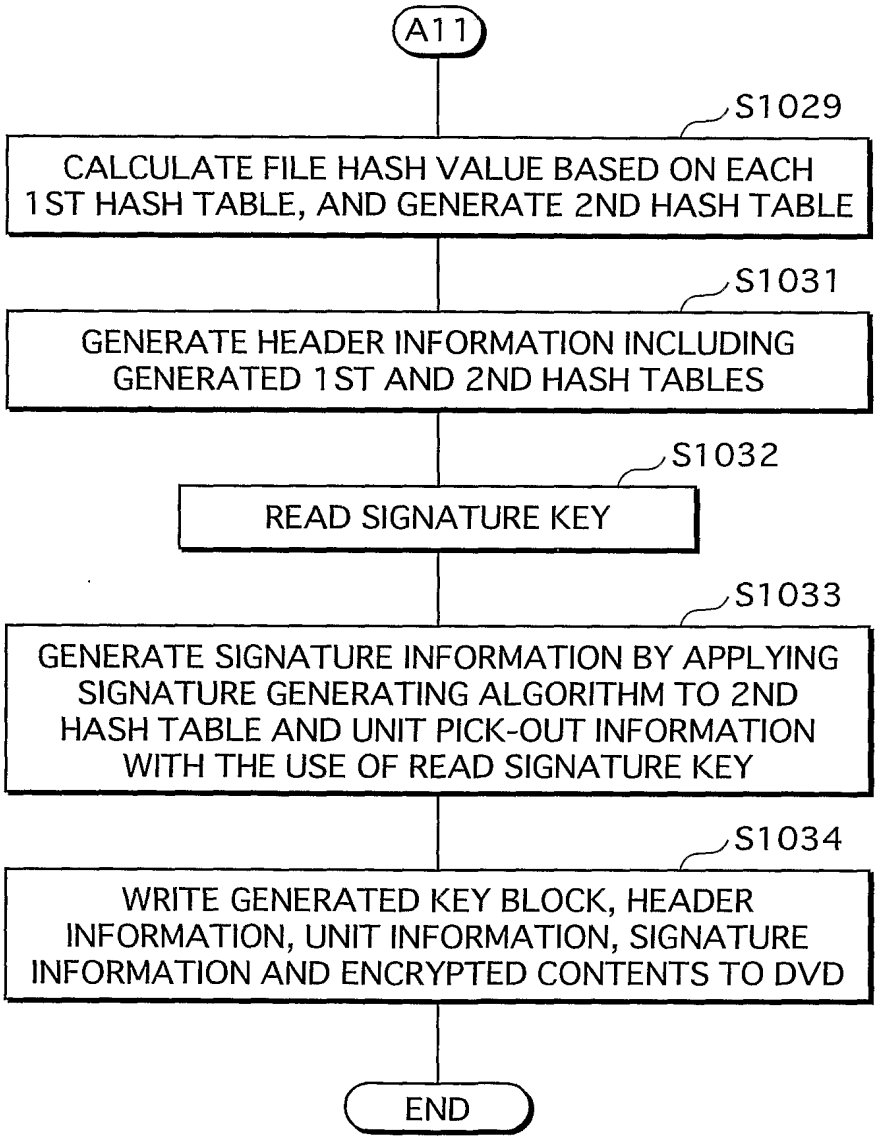

A11
S1029
CALCULATE FILE HASH VALUE BASED ON EACH 1ST HASH TABLE, AND GENERATE 2ND HASH TABLE
S1031
GENERATE HEADER INFORMATION INCLUDING GENERATED 1ST AND 2ND HASH TABLES
S1032
READ SIGNATURE KEY
S1033
GENERATE SIGNATURE INFORMATION BY APPLYING SIGNATURE GENERATING ALGORITHM TO 2ND HASH TABLE AND UNIT PICK-OUT INFORMATION WITH THE USE OF READ SIGNATURE KEY
S1034
WRITE GENERATED KEY BLOCK, HEADER INFORMATION, UNIT INFORMATION, SIGNATURE INFORMATION AND ENCRYPTED CONTENTS TO DVD
END

FIG.23

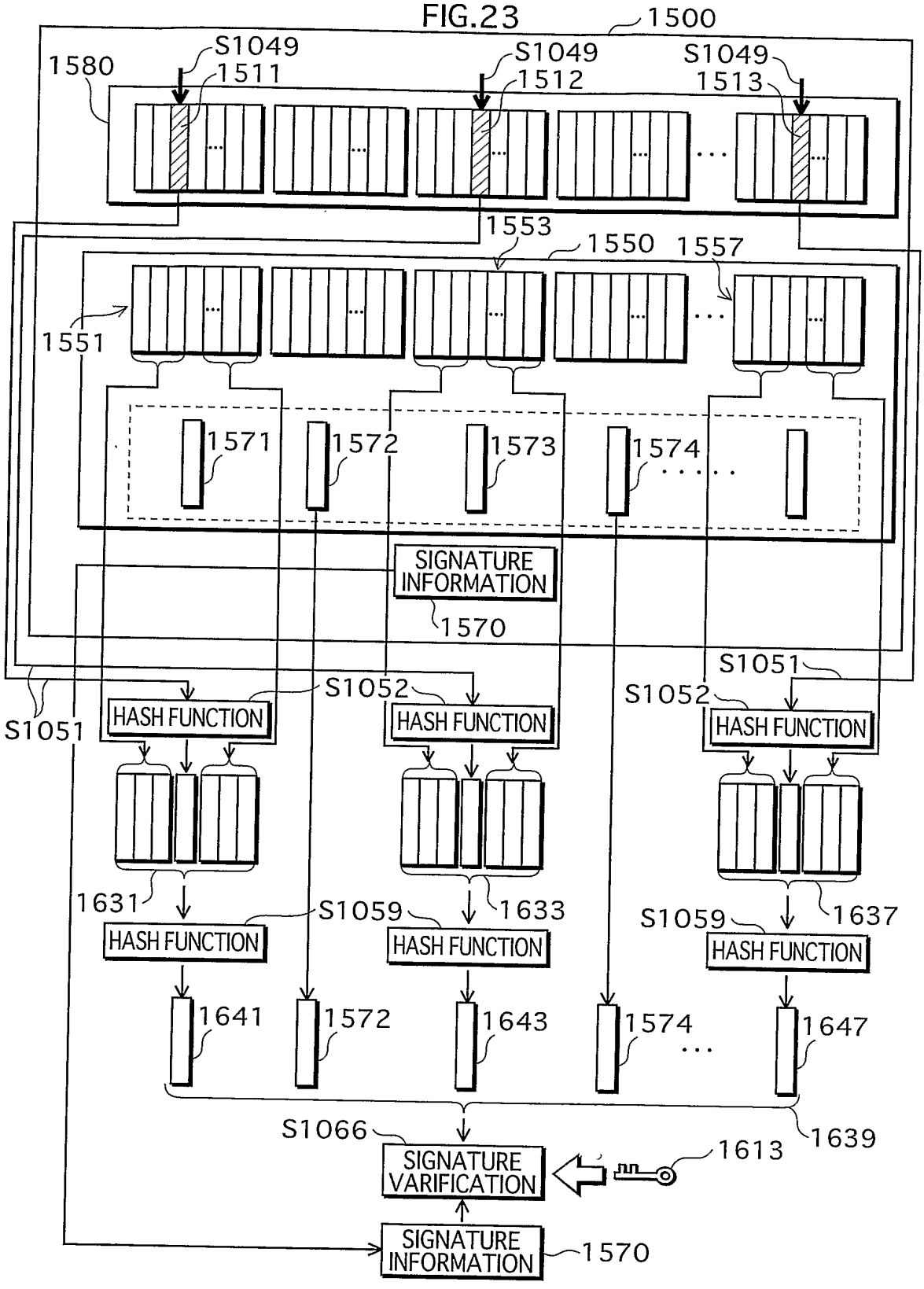

1500
1580
S1049
1511
S1049
1512
S1049
1513
1553
1550
1557
1551
1571
1572
1573
1574
SIGNATURE INFORMATION
1570
S1051
S1052
S1051
S1052
HASH FUNCTION
HASH FUNCTION
HASH FUNCTION
1631
1633
1637
S1059
S1059
HASH FUNCTION
HASH FUNCTION
HASH FUNCTION
1641
1572
1643
1574
1647
1639
S1066
SIGNATURE VARIFICATION
1613
SIGNATURE INFORMATION
1570

FIG.24

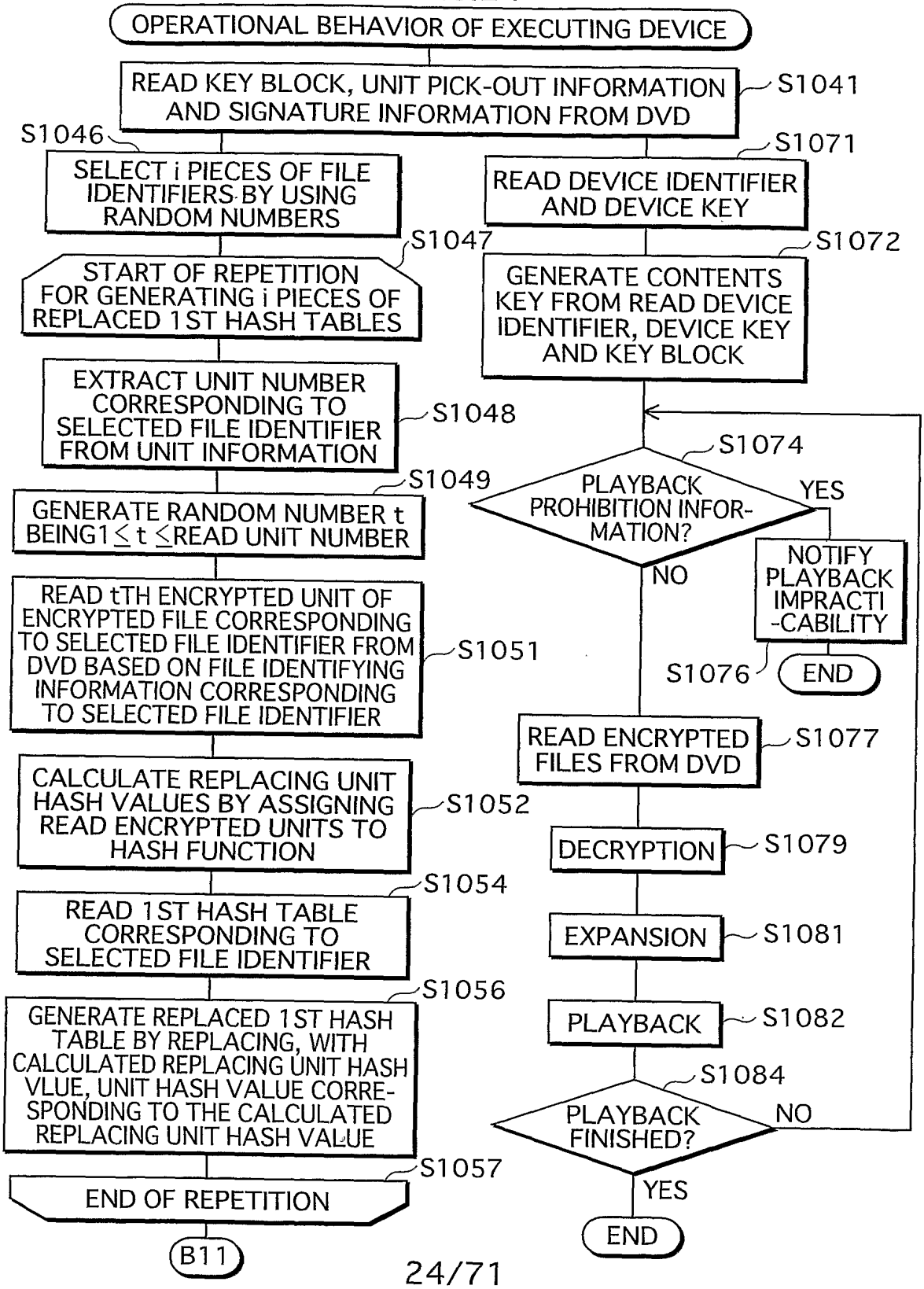

OPERATIONAL BEHAVIOR OF EXECUTING DEVICE
READ KEY BLOCK, UNIT PICK-OUT INFORMATION AND SIGNATURE INFORMATION FROM DVD
S1041
S1046
SELECT i PIECES OF FILE IDENTIFIERS BY USING RANDOM NUMBERS
S1047
START OF REPETITION FOR GENERATING i PIECES OF REPLACED 1ST HASH TABLES
EXTRACT UNIT NUMBER CORRESPONDING TO SELECTED FILE IDENTIFIER FROM UNIT INFORMATION
S1048
S1049
GENERATE RANDOM NUMBER t BEING1 ≤ t ≤READ UNIT NUMBER
READ tTH ENCRYPTED UNIT OF ENCRYPTED FILE CORRESPONDING TO SELECTED FILE IDENTIFIER FROM DVD BASED ON FILE IDENTIFYING INFORMATION CORRESPONDING TO SELECTED FILE IDENTIFIER
S1051
CALCULATE REPLACING UNIT HASH VALUES BY ASSIGNING READ ENCRYPTED UNITS TO HASH FUNCTION
S1052
S1054
READ 1ST HASH TABLE CORRESPONDING TO SELECTED FILE IDENTIFIER
S1056
GENERATE REPLACED 1ST HASH TABLE BY REPLACING, WITH CALCULATED REPLACING UNIT HASH VLUE, UNIT HASH VALUE CORRESPONDING TO THE CALCULATED REPLACING UNIT HASH VALUE
S1057
END OF REPETITION
B11
S1071
READ DEVICE IDENTIFIER AND DEVICE KEY
S1072
GENERATE CONTENTS KEY FROM READ DEVICE IDENTIFIER, DEVICE KEY AND KEY BLOCK
S1074
PLAYBACK PROHIBITION INFORMATION?
YES
NO
NOTIFY PLAYBACK IMPRACTICABILITY
S1076
END
READ ENCRYPTED FILES FROM DVD
S1077
DECRYPTION
S1079
EXPANSION
S1081
PLAYBACK
S1082
S1084
PLAYBACK FINISHED?
NO
YES
END

FIG.25

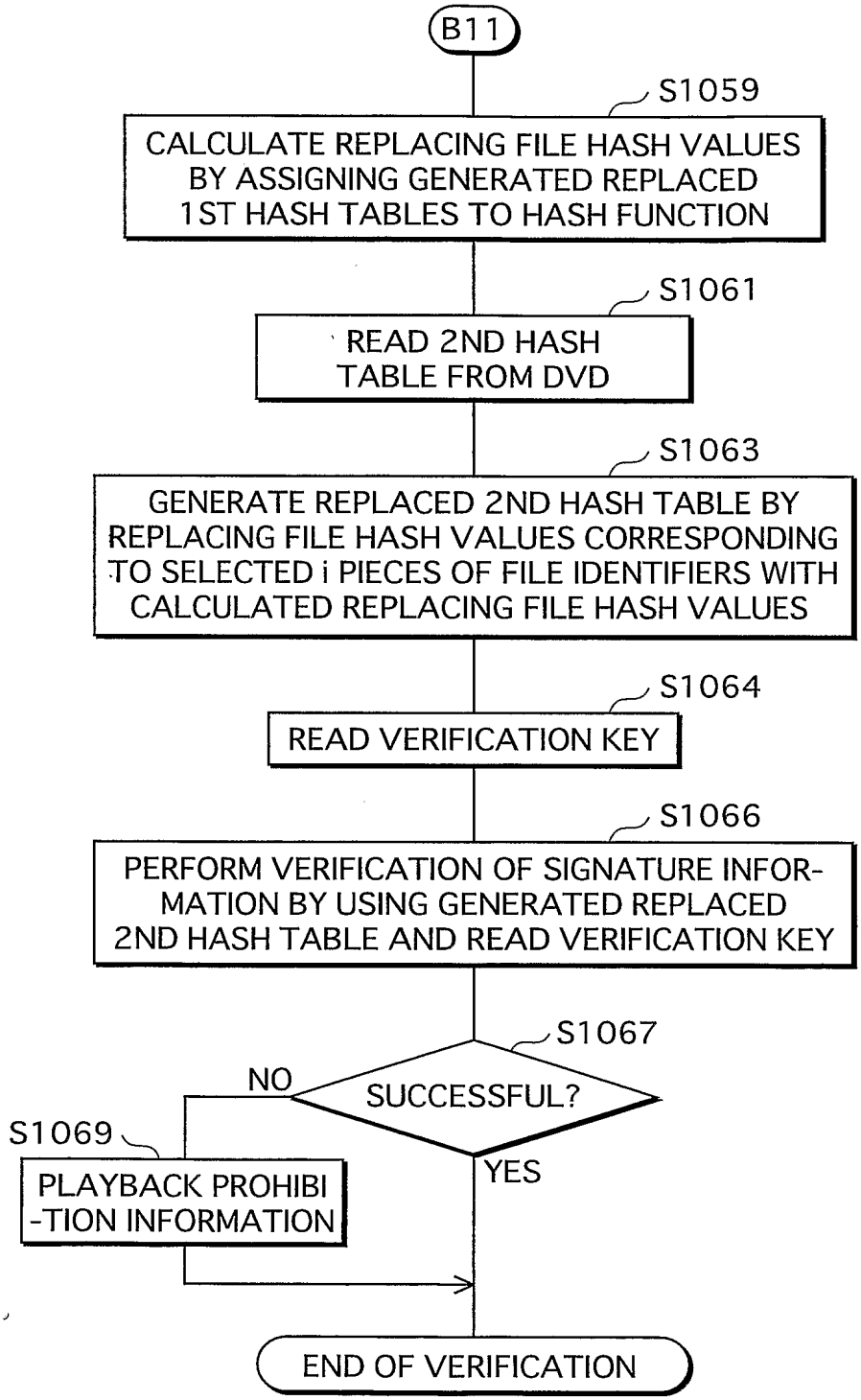

B11
S1059
CALCULATE REPLACING FILE HASH VALUES BY ASSIGNING GENERATED REPLACED 1ST HASH TABLES TO HASH FUNCTION
S1061
READ 2ND HASH TABLE FROM DVD
S1063
GENERATE REPLACED 2ND HASH TABLE BY REPLACING FILE HASH VALUES CORRESPONDING TO SELECTED i PIECES OF FILE IDENTIFIERS WITH CALCULATED REPLACING FILE HASH VALUES
S1064
READ VERIFICATION KEY
S1066
PERFORM VERIFICATION OF SIGNATURE INFOR-MATION BY USING GENERATED REPLACED 2ND HASH TABLE AND READ VERIFICATION KEY
S1067
SUCCESSFUL?
NO
YES
S1069
PLAYBACK PROHIBI -TION INFORMATION
END OF VERIFICATION

FIG.26

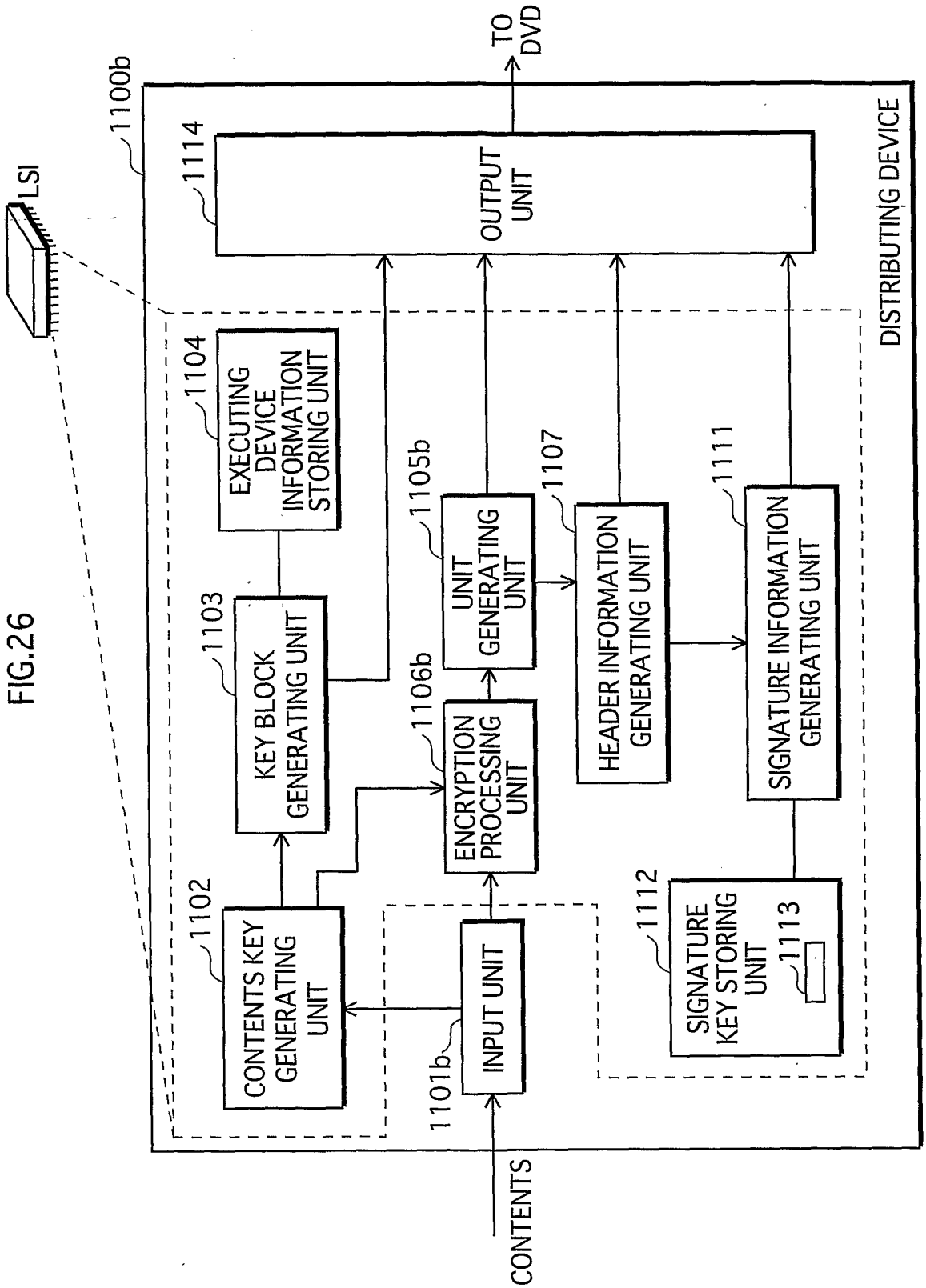

LSI
1100b
DISTRIBUTING DEVICE
TO DVD
1114
OUTPUT UNIT
1104
EXECUTING DEVICE INFORMATION STORING UNIT
1103
KEY BLOCK GENERATING UNIT
1105b
UNIT GENERATING UNIT
1107
HEADER INFORMATION GENERATING UNIT
1111
SIGNATURE INFORMATION GENERATING UNIT
1106b
ENCRYPTION PROCESSING UNIT
1102
CONTENTS KEY GENERATING UNIT
1101b
INPUT UNIT
1112
SIGNATURE KEY STORING UNIT
1113
CONTENTS

FIG.27

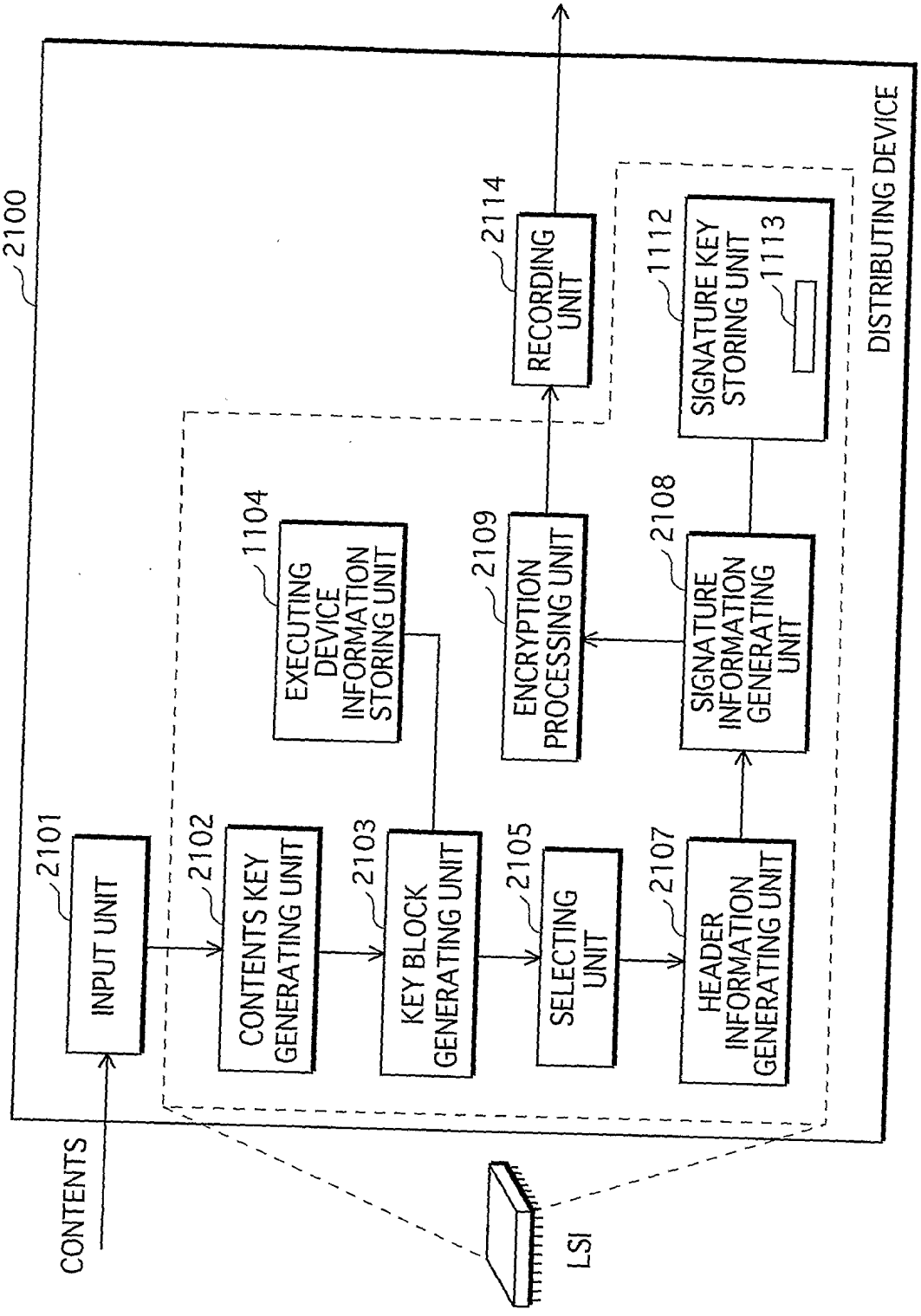

2100
DISTRIBUTING DEVICE
2101
INPUT UNIT
2102
CONTENTS KEY GENERATING UNIT
2103
KEY BLOCK GENERATING UNIT
2105
SELECTING UNIT
2107
HEADER INFORMATION GENERATING UNIT
1104
EXECUTING DEVICE INFORMATION STORING UNIT
2109
ENCRYPTION PROCESSING UNIT
2108
SIGNATURE INFORMATION GENERATING UNIT
2114
RECORDING UNIT
1112
SIGNATURE KEY STORING UNIT
1113
CONTENTS
LSI

FIG.28

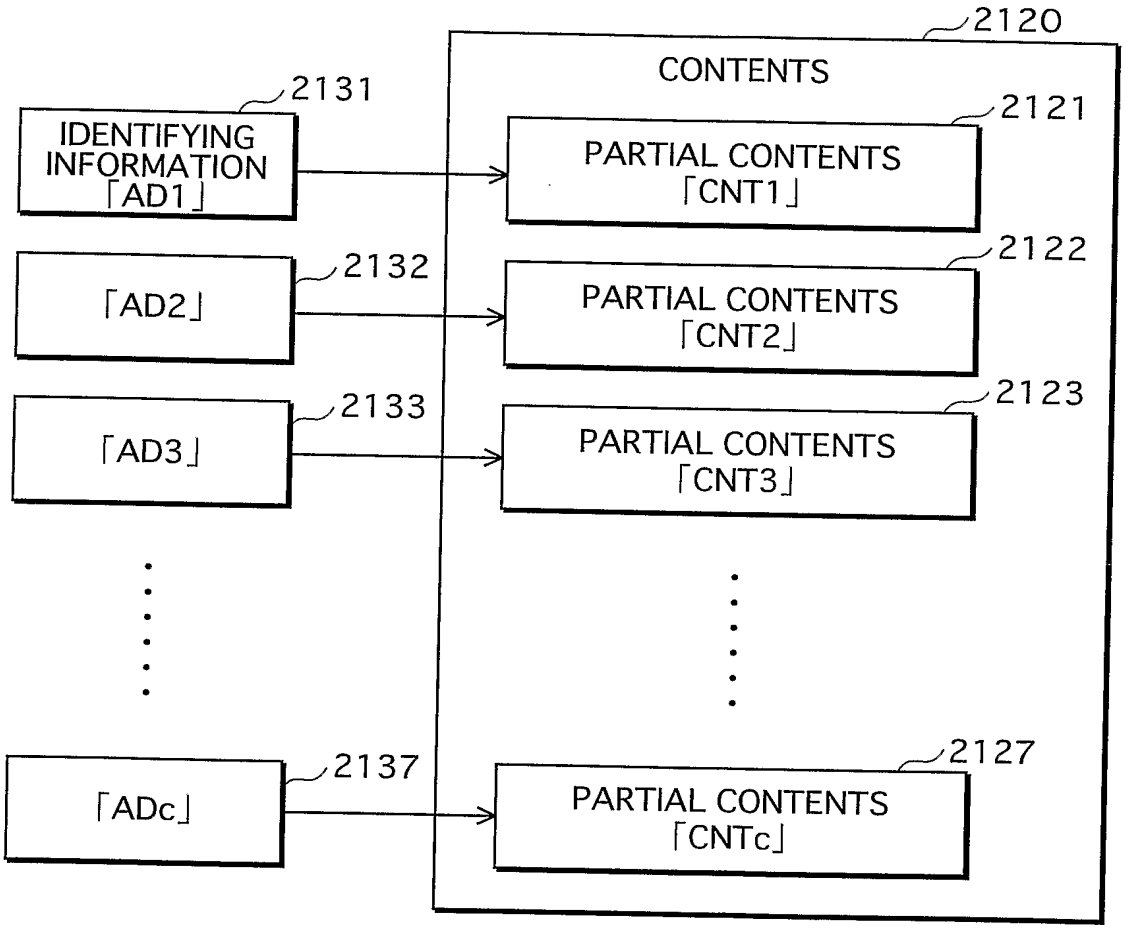

2120
CONTENTS
2131
IDENTIFYING INFORMATION 「AD1」
2121
PARTIAL CONTENTS 「CNT1」
2132
「AD2」
2122
PARTIAL CONTENTS 「CNT2」
2133
「AD3」
2123
PARTIAL CONTENTS 「CNT3」
2137
「ADc」
2127
PARTIAL CONTENTS 「CNTc」

FIG.29

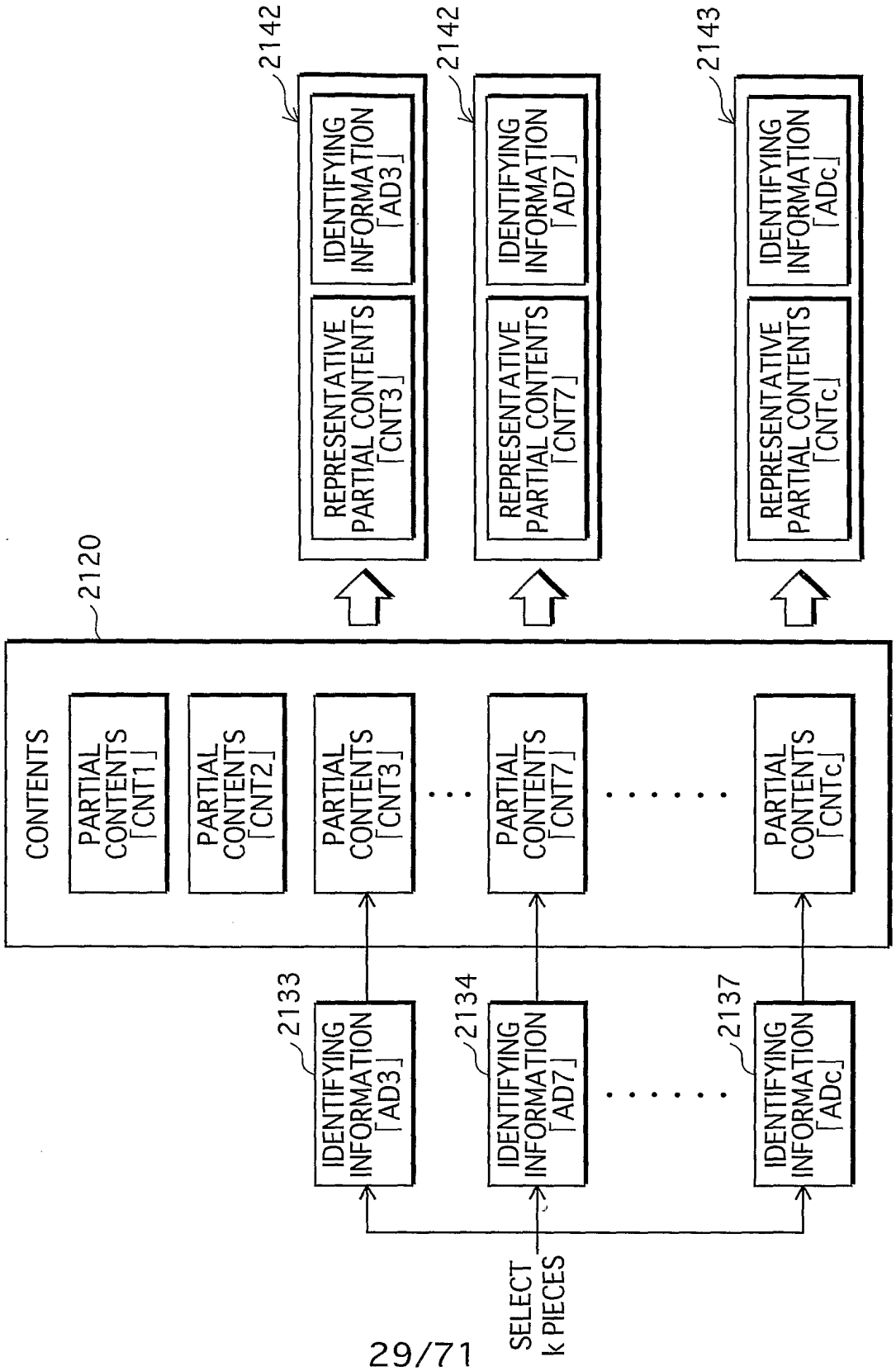

2142
2142
2143
IDENTIFYING INFORMATION 「AD3」
IDENTIFYING INFORMATION 「AD7」
IDENTIFYING INFORMATION 「ADc」
REPRESENTATIVE PARTIAL CONTENTS 「CNT3」
REPRESENTATIVE PARTIAL CONTENTS 「CNT7」
REPRESENTATIVE PARTIAL CONTENTS 「CNTc」
2120
CONTENTS
PARTIAL CONTENTS 「CNT1」
PARTIAL CONTENTS 「CNT2」
PARTIAL CONTENTS 「CNT3」
PARTIAL CONTENTS 「CNT7」
PARTIAL CONTENTS 「CNTc」
2133
2134
2137
IDENTIFYING INFORMATION 「AD3」
IDENTIFYING INFORMATION 「AD7」
IDENTIFYING INFORMATION 「ADc」
SELECT k PIECES

FIG.30

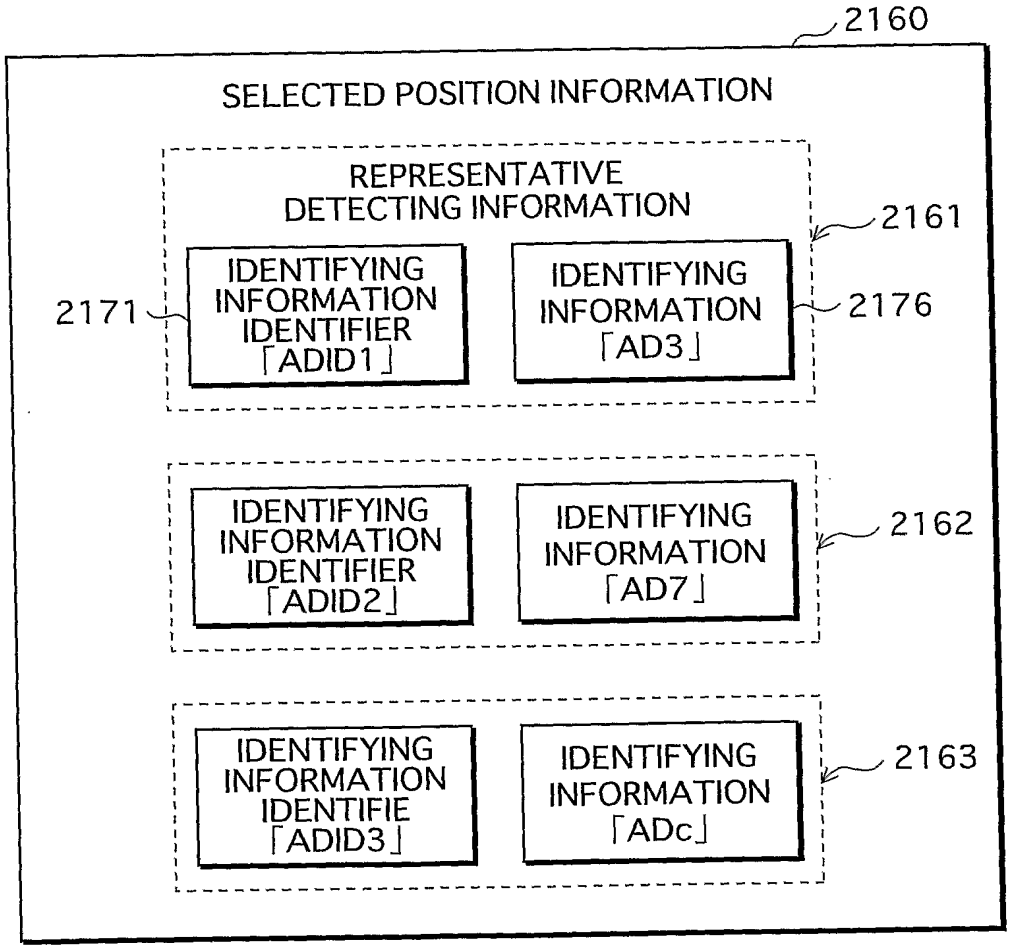

2160
SELECTED POSITION INFORMATION
REPRESENTATIVE DETECTING INFORMATION
2161
2171
IDENTIFYING INFORMATION IDENTIFIER 「ADID1」
IDENTIFYING INFORMATION 「AD3」
2176
IDENTIFYING INFORMATION IDENTIFIER 「ADID2」
IDENTIFYING INFORMATION 「AD7」
2162
IDENTIFYING INFORMATION IDENTIFIE 「ADID3」
IDENTIFYING INFORMATION 「ADc」
2163

FIG.31

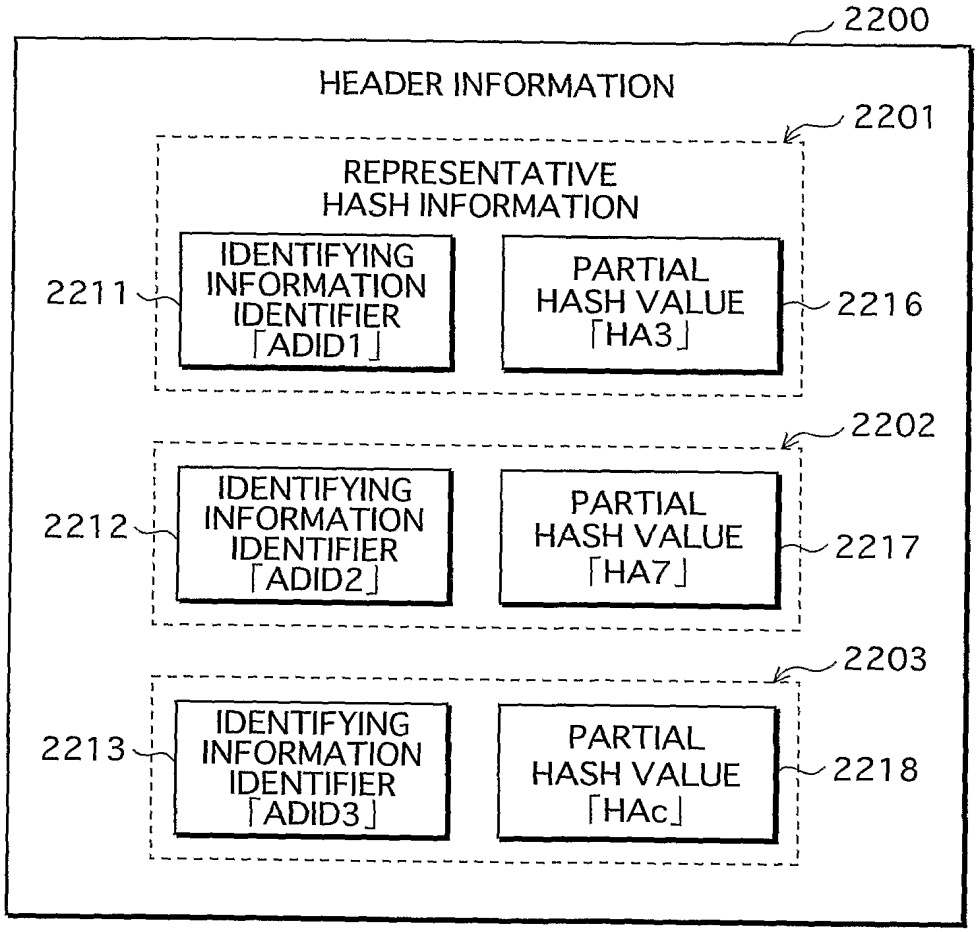

2200
HEADER INFORMATION
2201
REPRESENTATIVE HASH INFORMATION
2211
IDENTIFYING INFORMATION IDENTIFIER 「ADID1」
PARTIAL HASH VALUE 「HA3」
2216
2202
2212
IDENTIFYING INFORMATION IDENTIFIER 「ADID2」
PARTIAL HASH VALUE 「HA7」
2217
2203
2213
IDENTIFYING INFORMATION IDENTIFIER 「ADID3」
PARTIAL HASH VALUE 「HAc」
2218

FIG.32

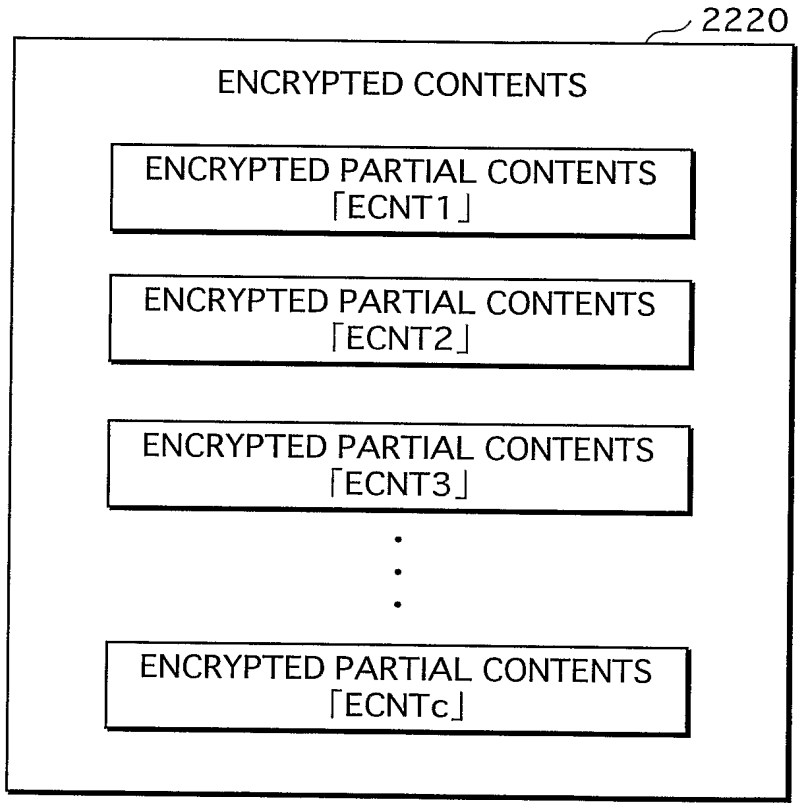

2220
ENCRYPTED CONTENTS
ENCRYPTED PARTIAL CONTENTS 「ECNT1」
ENCRYPTED PARTIAL CONTENTS 「ECNT2」
ENCRYPTED PARTIAL CONTENTS 「ECNT3」
ENCRYPTED PARTIAL CONTENTS 「ECNTc」

FIG.33

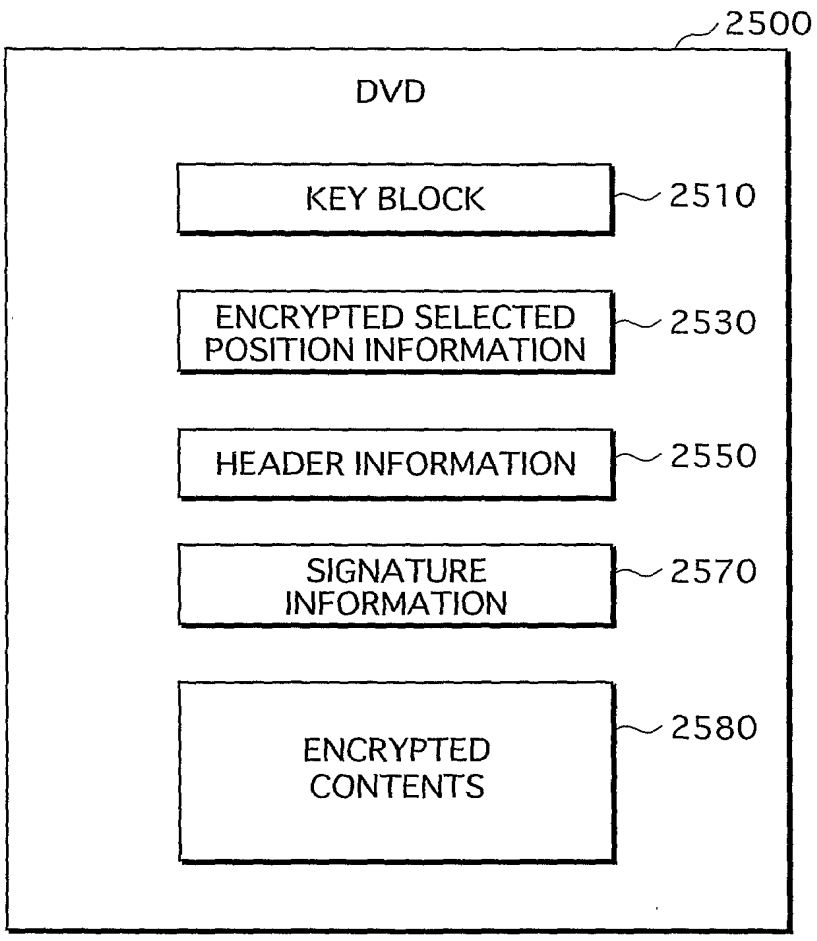

2500
DVD
KEY BLOCK
2510
ENCRYPTED SELECTED POSITION INFORMATION
2530
HEADER INFORMATION
2550
SIGNATURE INFORMATION
2570
ENCRYPTED CONTENTS
2580

FIG.34

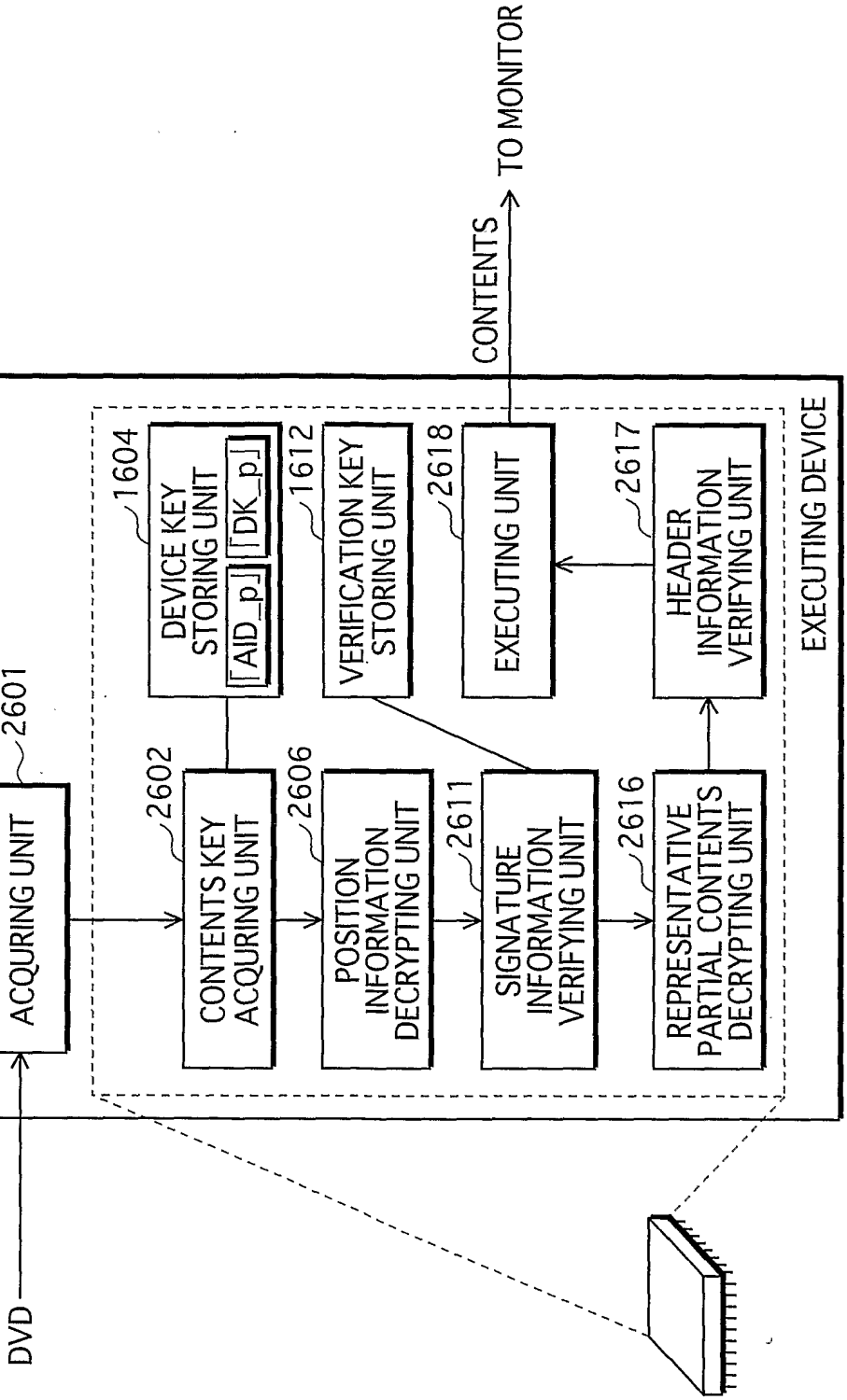

2600
EXECUTING DEVICE
ACQURING UNIT
2601
CONTENTS KEY ACQURING UNIT
2602
DEVICE KEY STORING UNIT
1604
「AID_p」
「DK_p」
1612
POSITION INFORMATION DECRYPTING UNIT
2606
VERIFICATION KEY STORING UNIT
SIGNATURE INFORMATION VERIFYING UNIT
2611
EXECUTING UNIT
2618
REPRESENTATIVE PARTIAL CONTENTS DECRYPTING UNIT
2616
HEADER INFORMATION VERIFYING UNIT
2617
CONTENTS
TO MONITOR
DVD

FIG.35

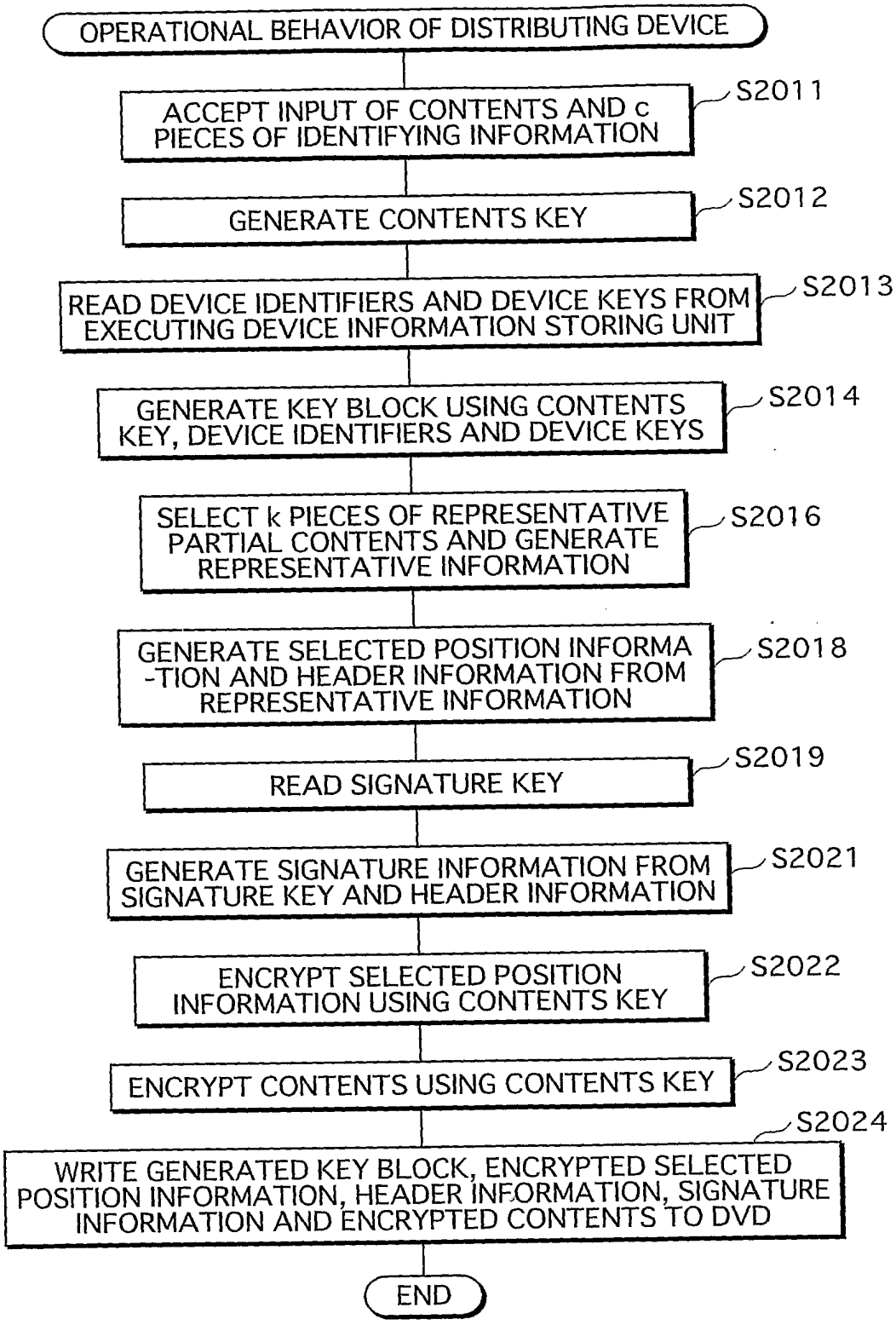

OPERATIONAL BEHAVIOR OF DISTRIBUTING DEVICE
ACCEPT INPUT OF CONTENTS AND c PIECES OF IDENTIFYING INFORMATION
S2011
GENERATE CONTENTS KEY
S2012
READ DEVICE IDENTIFIERS AND DEVICE KEYS FROM EXECUTING DEVICE INFORMATION STORING UNIT
S2013
GENERATE KEY BLOCK USING CONTENTS KEY, DEVICE IDENTIFIERS AND DEVICE KEYS
S2014
SELECT k PIECES OF REPRESENTATIVE PARTIAL CONTENTS AND GENERATE REPRESENTATIVE INFORMATION
S2016
GENERATE SELECTED POSITION INFORMA -TION AND HEADER INFORMATION FROM REPRESENTATIVE INFORMATION
S2018
READ SIGNATURE KEY
S2019
GENERATE SIGNATURE INFORMATION FROM SIGNATURE KEY AND HEADER INFORMATION
S2021
ENCRYPT SELECTED POSITION INFORMATION USING CONTENTS KEY
S2022
ENCRYPT CONTENTS USING CONTENTS KEY
S2023
WRITE GENERATED KEY BLOCK, ENCRYPTED SELECTED POSITION INFORMATION, HEADER INFORMATION, SIGNATURE INFORMATION AND ENCRYPTED CONTENTS TO DVD
S2024
END

FIG.36

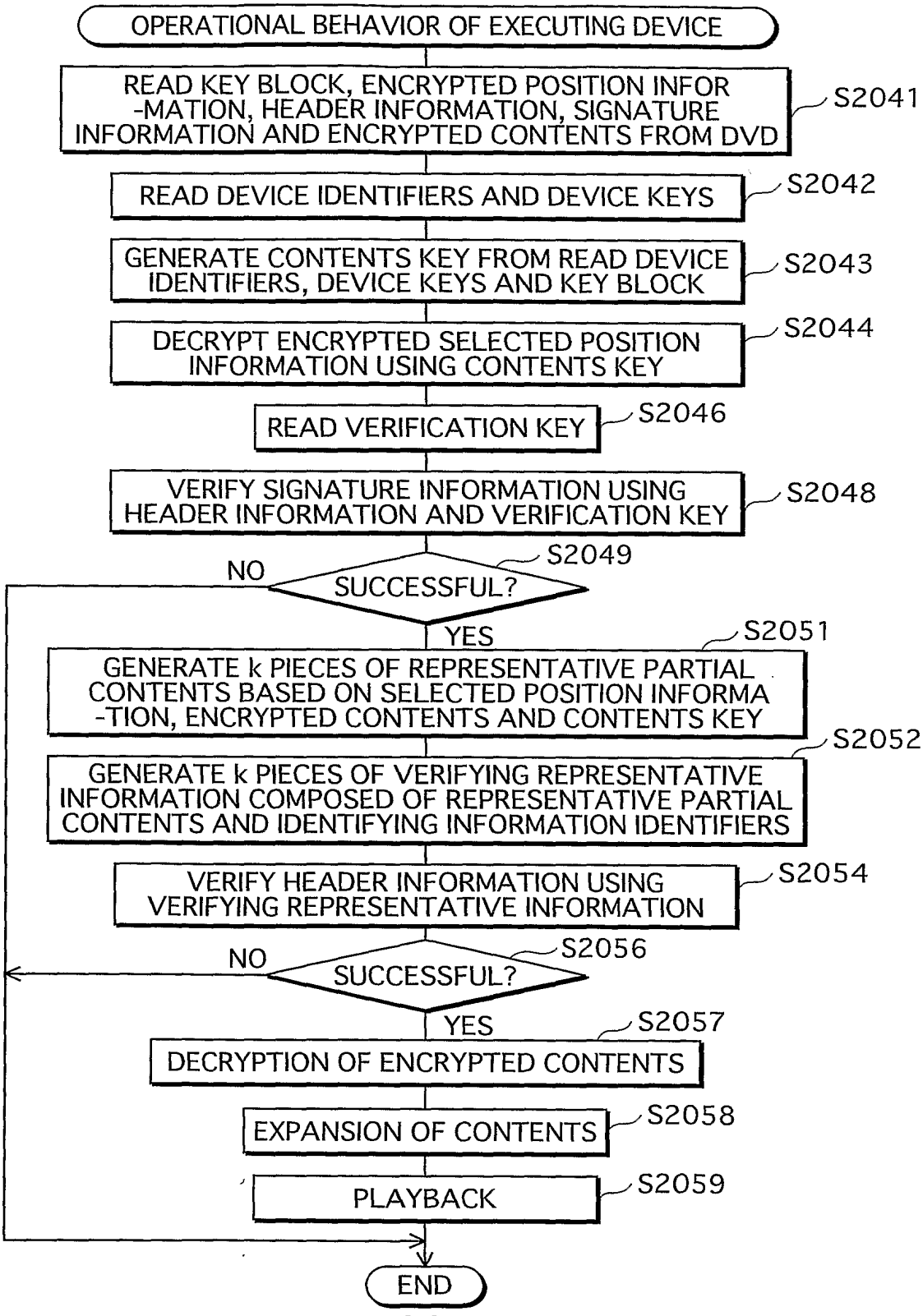

OPERATIONAL BEHAVIOR OF EXECUTING DEVICE
READ KEY BLOCK, ENCRYPTED POSITION INFOR -MATION, HEADER INFORMATION, SIGNATURE INFORMATION AND ENCRYPTED CONTENTS FROM DVD
S2041
READ DEVICE IDENTIFIERS AND DEVICE KEYS
S2042
GENERATE CONTENTS KEY FROM READ DEVICE IDENTIFIERS, DEVICE KEYS AND KEY BLOCK
S2043
DECRYPT ENCRYPTED SELECTED POSITION INFORMATION USING CONTENTS KEY
S2044
READ VERIFICATION KEY
S2046
VERIFY SIGNATURE INFORMATION USING HEADER INFORMATION AND VERIFICATION KEY
S2048
SUCCESSFUL?
S2049
NO
YES
GENERATE k PIECES OF REPRESENTATIVE PARTIAL CONTENTS BASED ON SELECTED POSITION INFORMA -TION, ENCRYPTED CONTENTS AND CONTENTS KEY
S2051
GENERATE k PIECES OF VERIFYING REPRESENTATIVE INFORMATION COMPOSED OF REPRESENTATIVE PARTIAL CONTENTS AND IDENTIFYING INFORMATION IDENTIFIERS
S2052
VERIFY HEADER INFORMATION USING VERIFYING REPRESENTATIVE INFORMATION
S2054
SUCCESSFUL?
S2056
NO
YES
DECRYPTION OF ENCRYPTED CONTENTS
S2057
EXPANSION OF CONTENTS
S2058
PLAYBACK
S2059
END

FIG.37

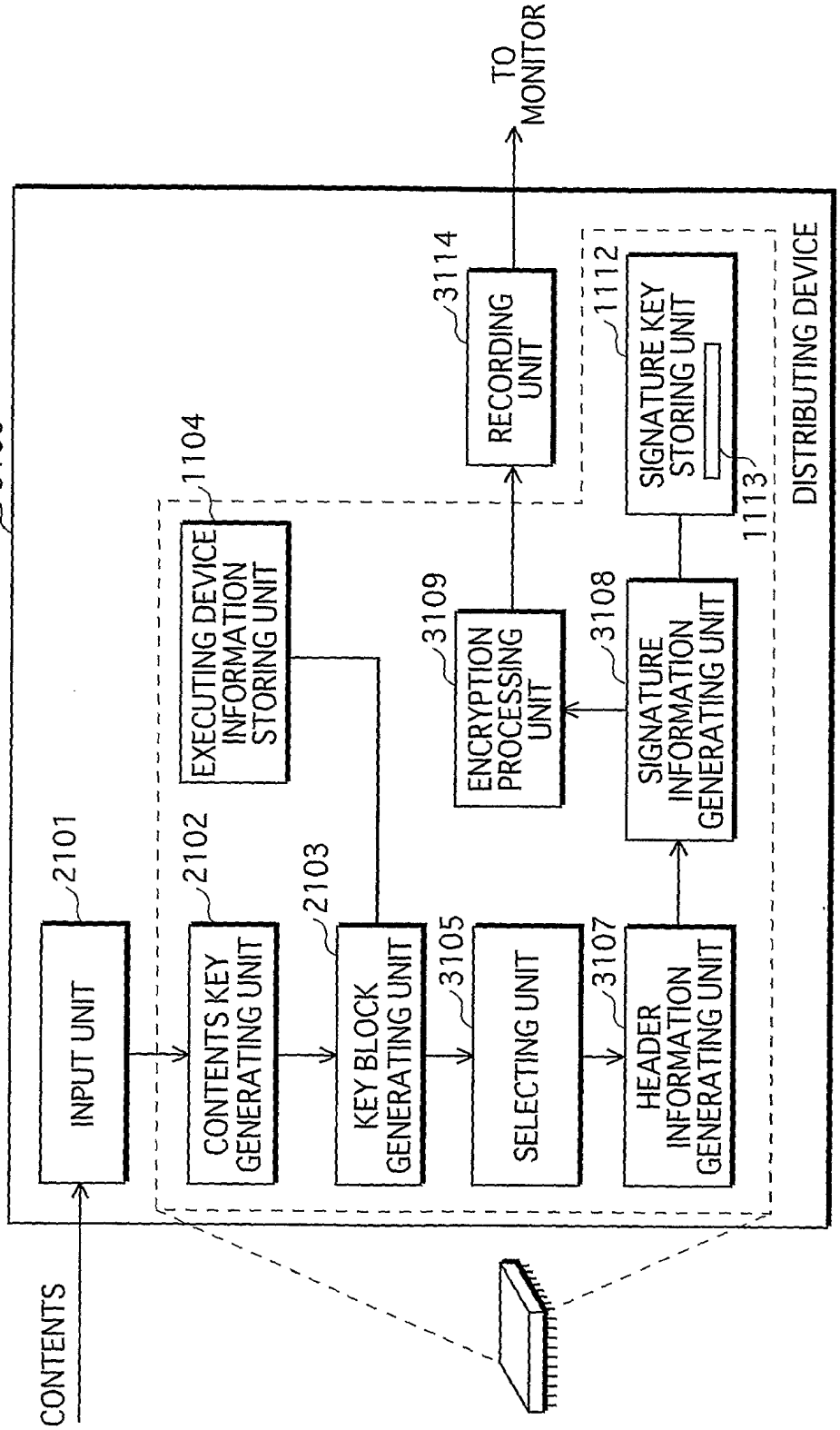

3100
DISTRIBUTING DEVICE
TO MONITOR
CONTENTS
INPUT UNIT
2101
CONTENTS KEY GENERATING UNIT
2102
KEY BLOCK GENERATING UNIT
2103
SELECTING UNIT
3105
HEADER INFORMATION GENERATING UNIT
3107
EXECUTING DEVICE INFORMATION STORING UNIT
1104
ENCRYPTION PROCESSING UNIT
3109
SIGNATURE INFORMATION GENERATING UNIT
3108
RECORDING UNIT
3114
SIGNATURE KEY STORING UNIT
1112
1113

FIG.38

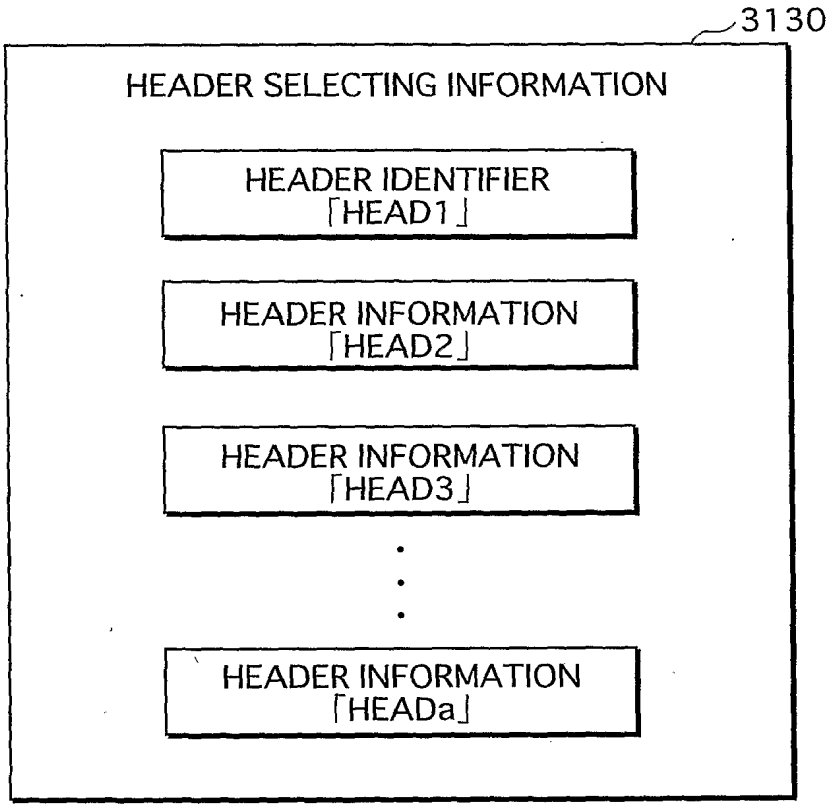

3130
HEADER SELECTING INFORMATION
HEADER IDENTIFIER
「HEAD1」
HEADER INFORMATION
「HEAD2」
HEADER INFORMATION
「HEAD3」
HEADER INFORMATION
「HEADa」

FIG.39

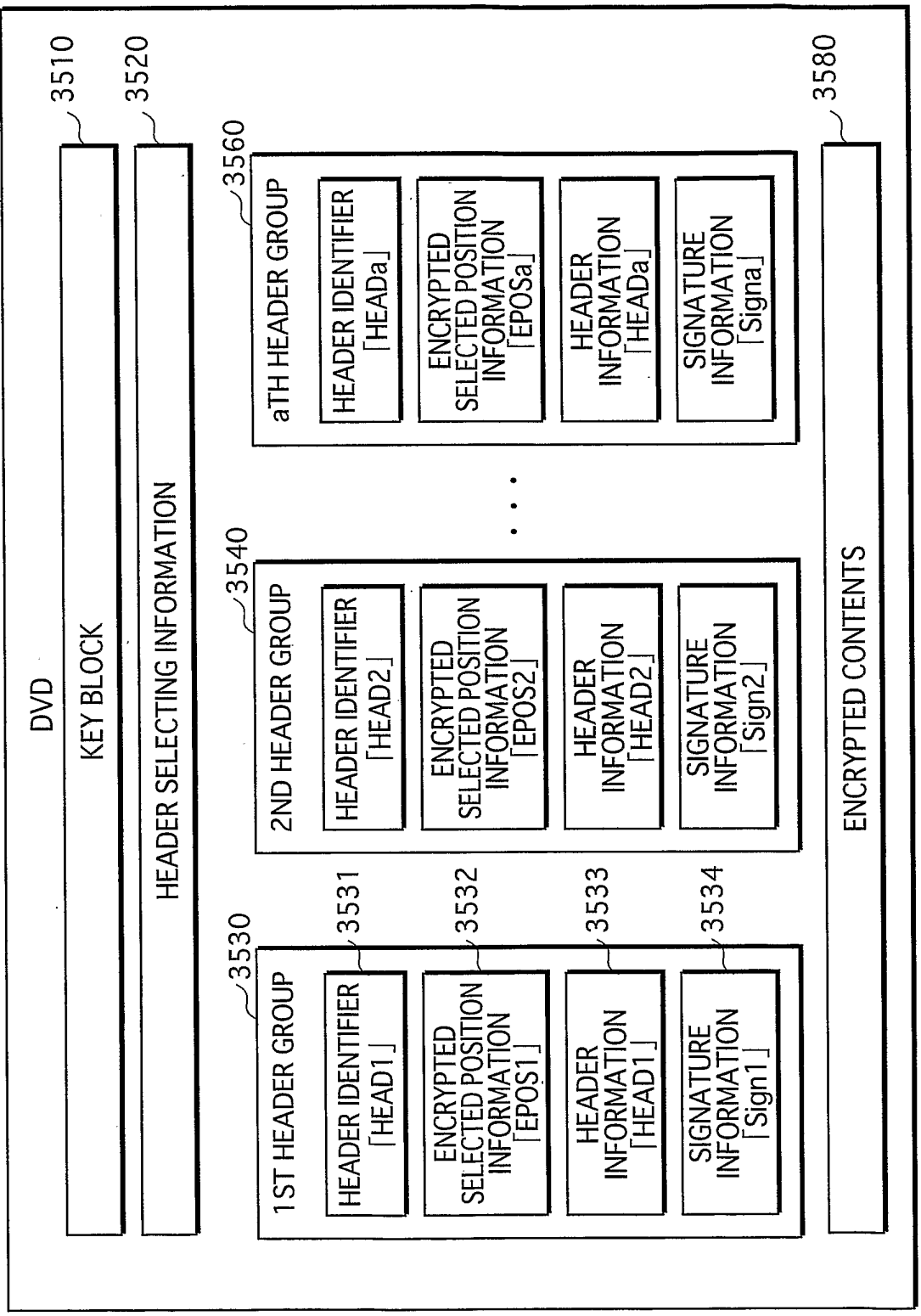

3500
DVD
3510
KEY BLOCK
3520
HEADER SELECTING INFORMATION
3530
1ST HEADER GROUP
3531
HEADER IDENTIFIER 「HEAD1」
3532
ENCRYPTED SELECTED POSITION INFORMATION 「EPOS1」
3533
HEADER INFORMATION 「HEAD1」
3534
SIGNATURE INFORMATION 「Sign1」
3540
2ND HEADER GROUP
HEADER IDENTIFIER 「HEAD2」
ENCRYPTED SELECTED POSITION INFORMATION 「EPOS2」
HEADER INFORMATION 「HEAD2」
SIGNATURE INFORMATION 「Sign2」
3560
aTH HEADER GROUP
HEADER IDENTIFIER 「HEADa」
ENCRYPTED SELECTED POSITION INFORMATION 「EPOSa」
HEADER INFORMATION 「HEADa」
SIGNATURE INFORMATION 「Signa」
3580
ENCRYPTED CONTENTS

FIG.40

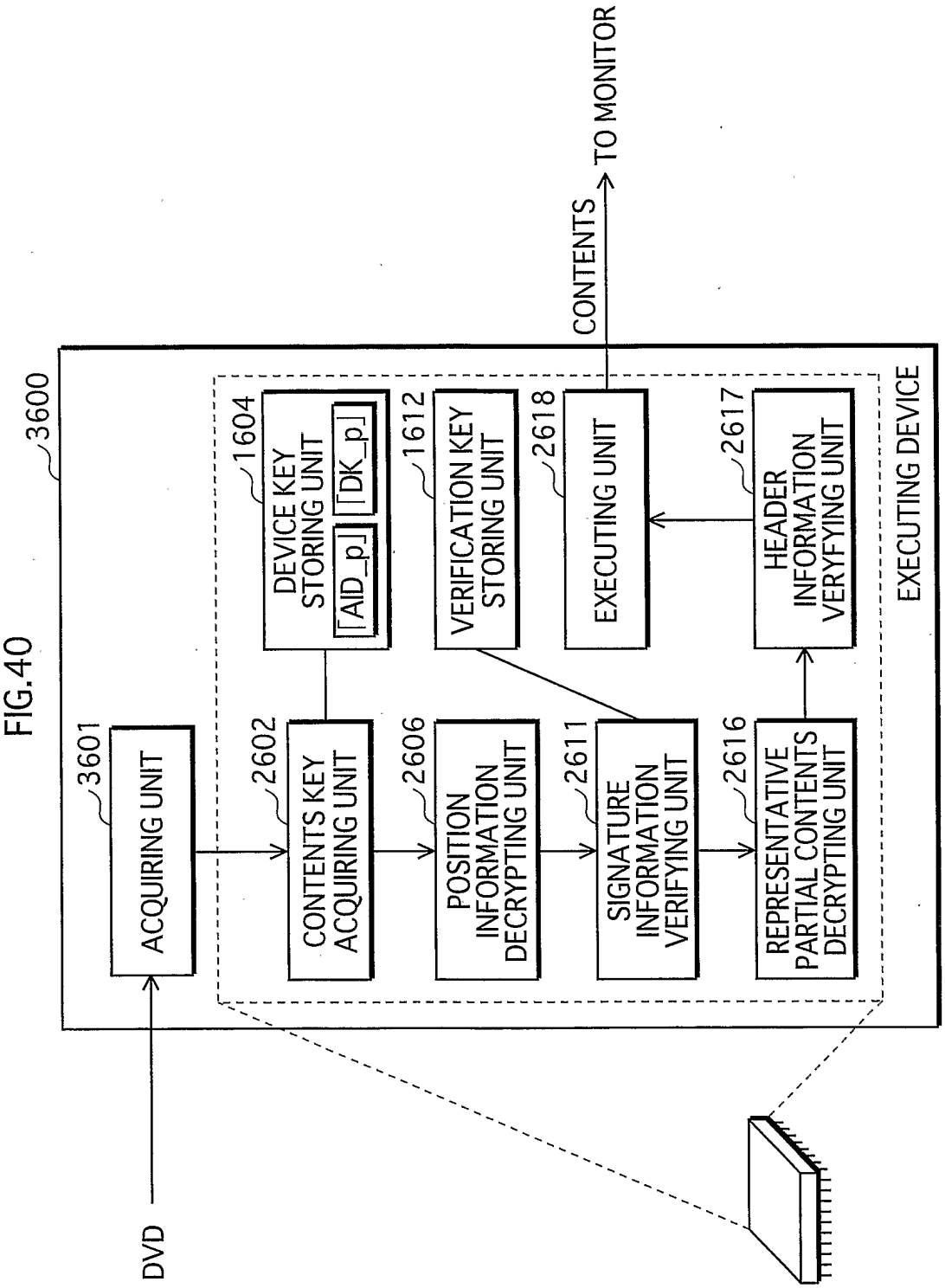

3600
EXECUTING DEVICE
1604
DEVICE KEY STORING UNIT
「AID_p」
「DK_p」
1612
VERIFICATION KEY STORING UNIT
2618
EXECUTING UNIT
2617
HEADER INFORMATION VERYFYING UNIT
3601
ACQUIRING UNIT
2602
CONTENTS KEY ACQUIRING UNIT
2606
POSITION INFORMATION DECRYPTING UNIT
2611
SIGNATURE INFORMATION VERIFYING UNIT
2616
REPRESENTATIVE PARTIAL CONTENTS DECRYPTING UNIT
CONTENTS
TO MONITOR
DVD

FIG.41

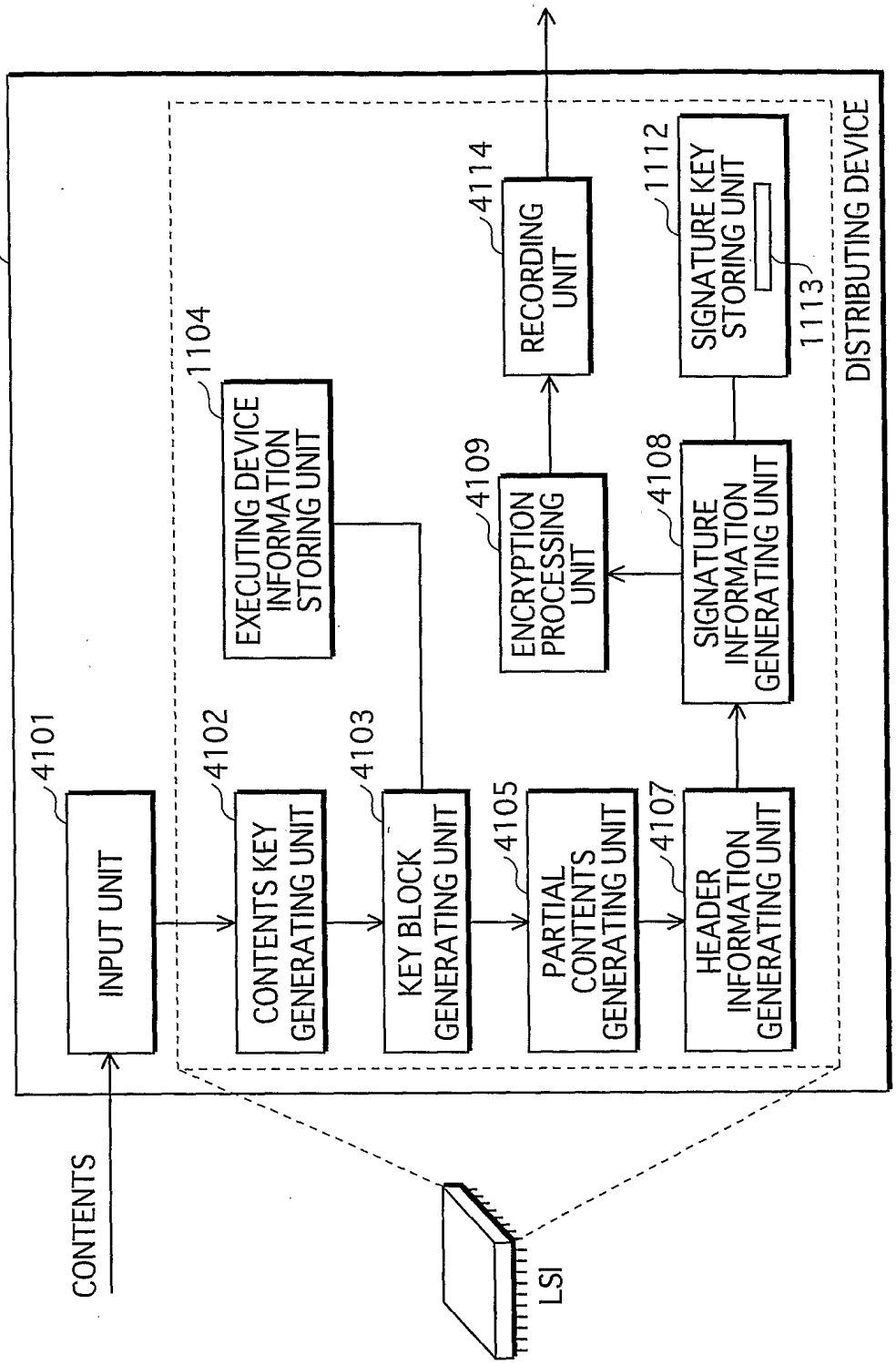

4100
DISTRIBUTING DEVICE
4101
INPUT UNIT
4102
CONTENTS KEY GENERATING UNIT
4103
KEY BLOCK GENERATING UNIT
4104
EXECUTING DEVICE INFORMATION STORING UNIT
4105
PARTIAL CONTENTS GENERATING UNIT
4107
HEADER INFORMATION GENERATING UNIT
4108
SIGNATURE INFORMATION GENERATING UNIT
4109
ENCRYPTION PROCESSING UNIT
4114
RECORDING UNIT
1112
SIGNATURE KEY STORING UNIT
1113
CONTENTS
LSI

FIG.42

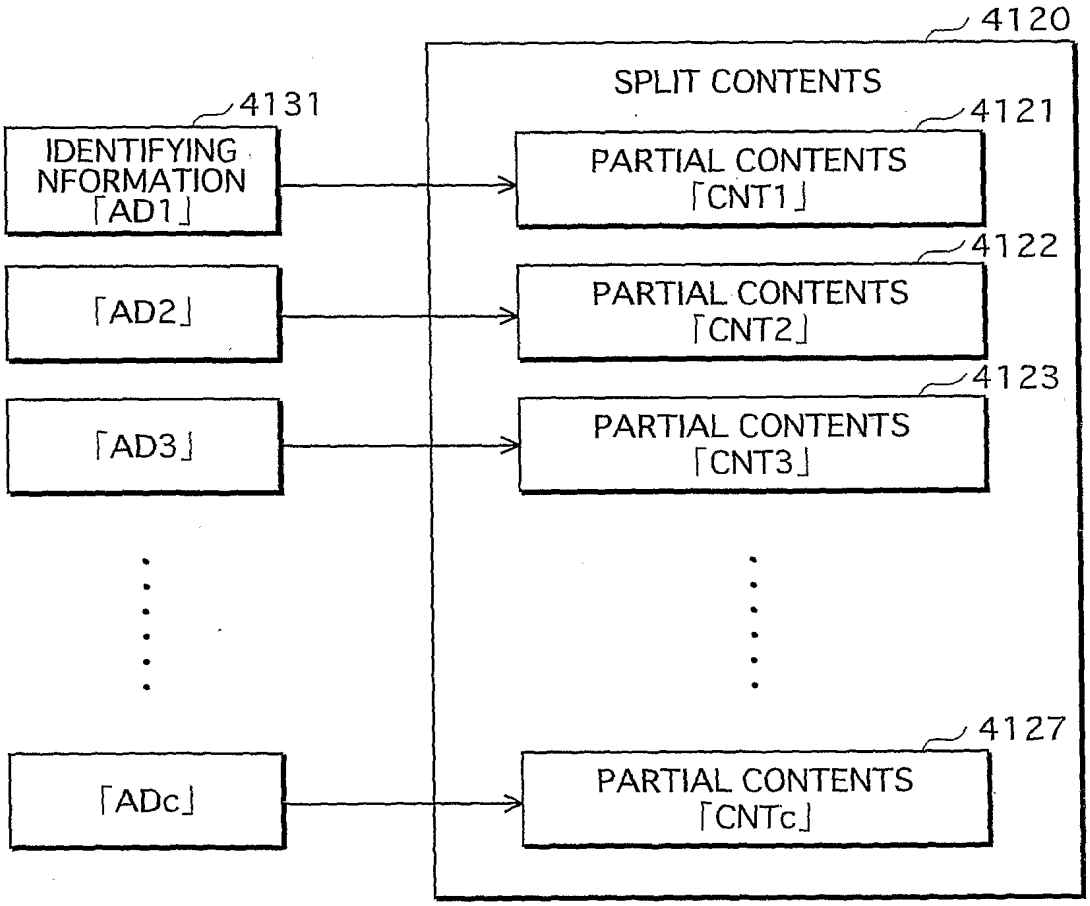

4120
SPLIT CONTENTS
4131
IDENTIFYING NFORMATION 「AD1」
4121
PARTIAL CONTENTS 「CNT1」
「AD2」
4122
PARTIAL CONTENTS 「CNT2」
「AD3」
4123
PARTIAL CONTENTS 「CNT3」
「ADc」
4127
PARTIAL CONTENTS 「CNTc」

FIG.43

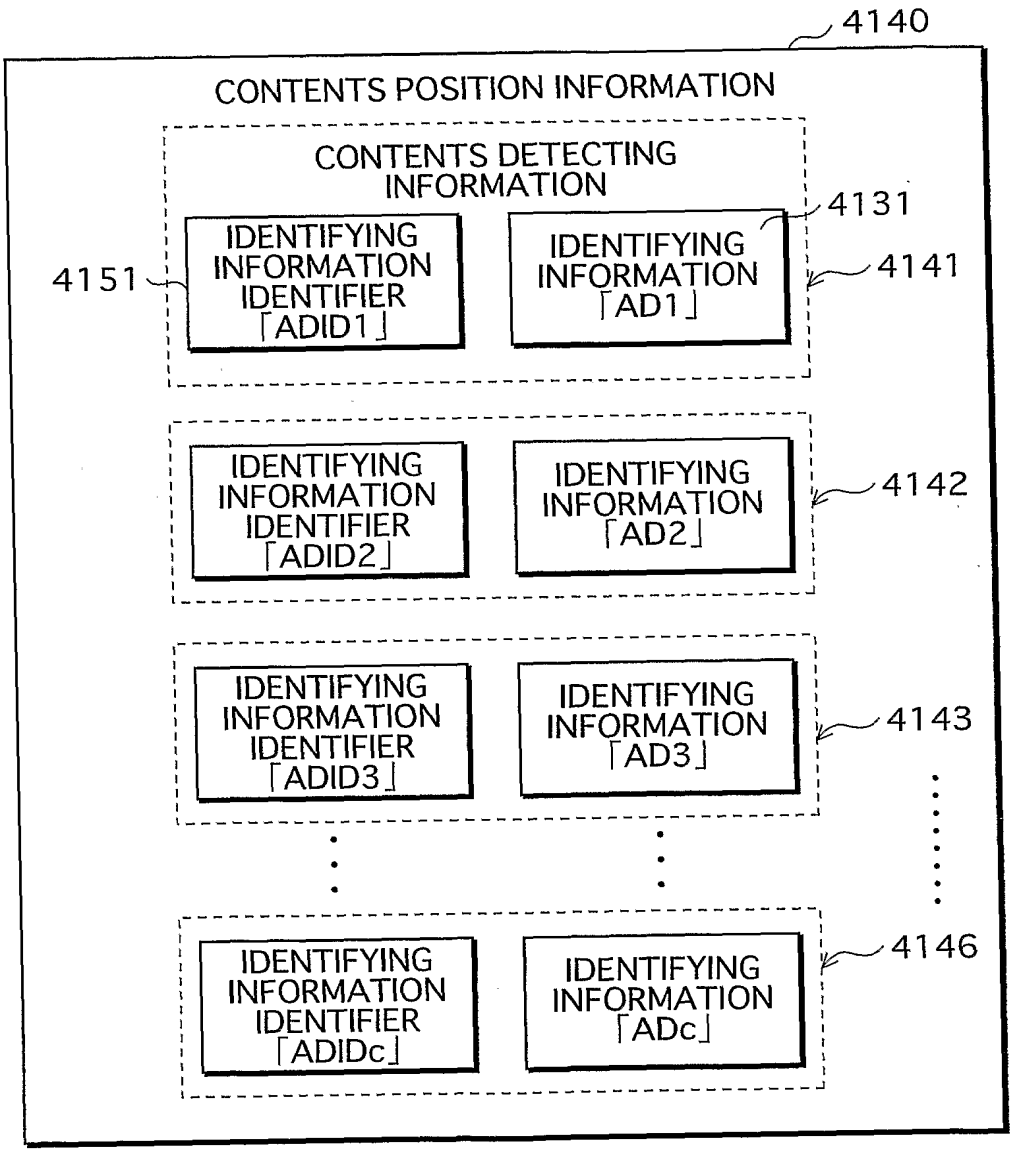

4140
CONTENTS POSITION INFORMATION
CONTENTS DETECTING INFORMATION
4131
4151
IDENTIFYING INFORMATION IDENTIFIER 「ADID1」
IDENTIFYING INFORMATION 「AD1」
4141
IDENTIFYING INFORMATION IDENTIFIER 「ADID2」
IDENTIFYING INFORMATION 「AD2」
4142
IDENTIFYING INFORMATION IDENTIFIER 「ADID3」
IDENTIFYING INFORMATION 「AD3」
4143
IDENTIFYING INFORMATION IDENTIFIER 「ADIDc」
IDENTIFYING INFORMATION 「ADc」
4146

FIG.44

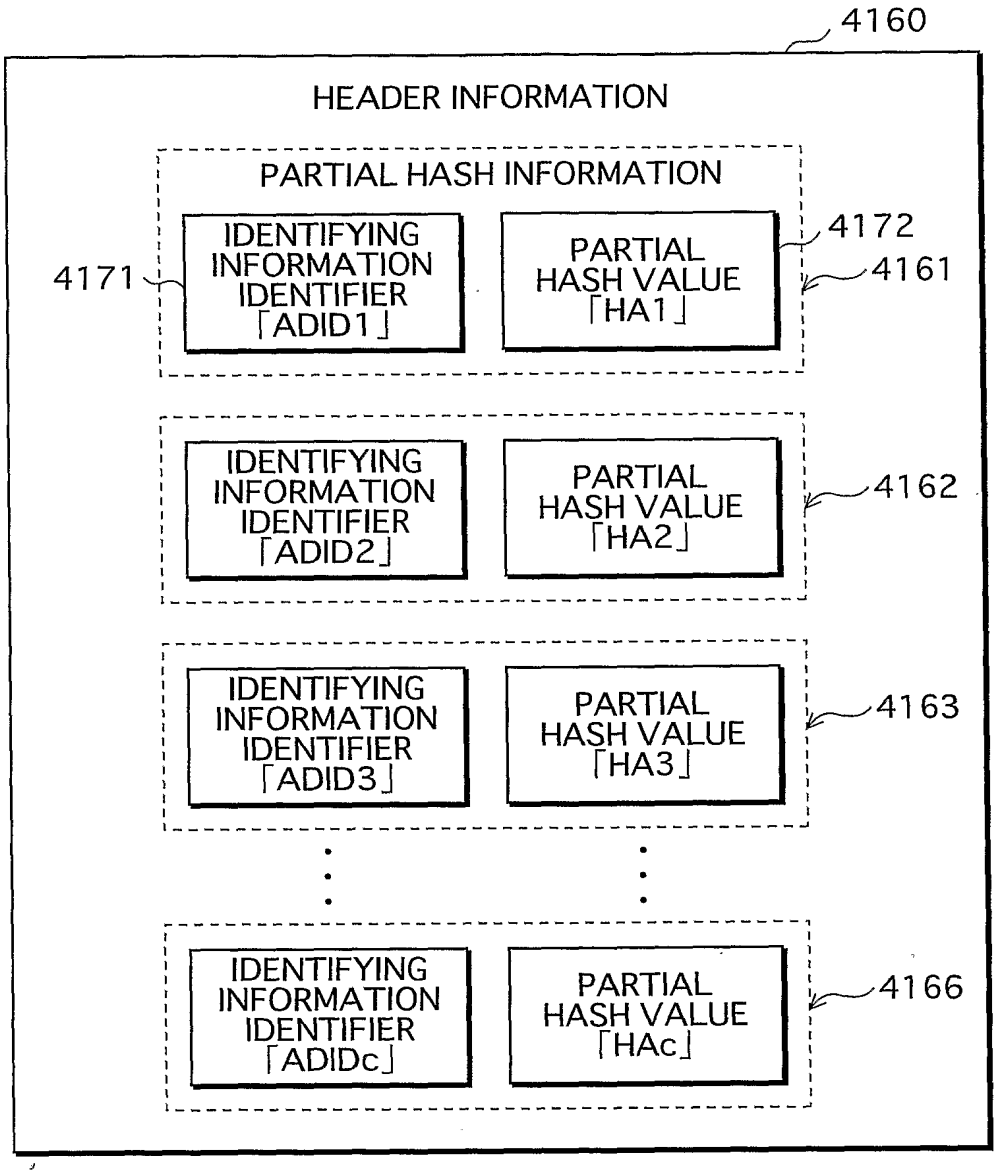

4160
HEADER INFORMATION
PARTIAL HASH INFORMATION
4171
IDENTIFYING INFORMATION IDENTIFIER 「ADID1」
PARTIAL HASH VALUE 「HA1」
4172
4161
IDENTIFYING INFORMATION IDENTIFIER 「ADID2」
PARTIAL HASH VALUE 「HA2」
4162
IDENTIFYING INFORMATION IDENTIFIER 「ADID3」
PARTIAL HASH VALUE 「HA3」
4163
IDENTIFYING INFORMATION IDENTIFIER 「ADIDc」
PARTIAL HASH VALUE 「HAc」
4166

FIG.45

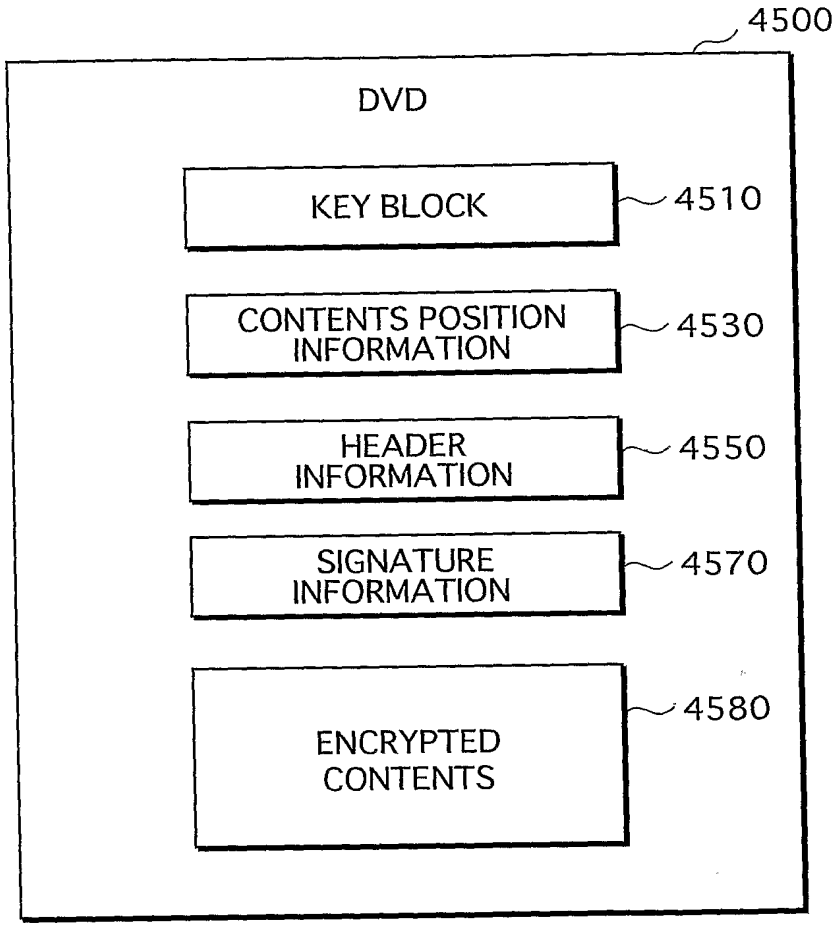

4500
DVD
KEY BLOCK
4510
CONTENTS POSITION INFORMATION
4530
HEADER INFORMATION
4550
SIGNATURE INFORMATION
4570
ENCRYPTED CONTENTS
4580

FIG.46

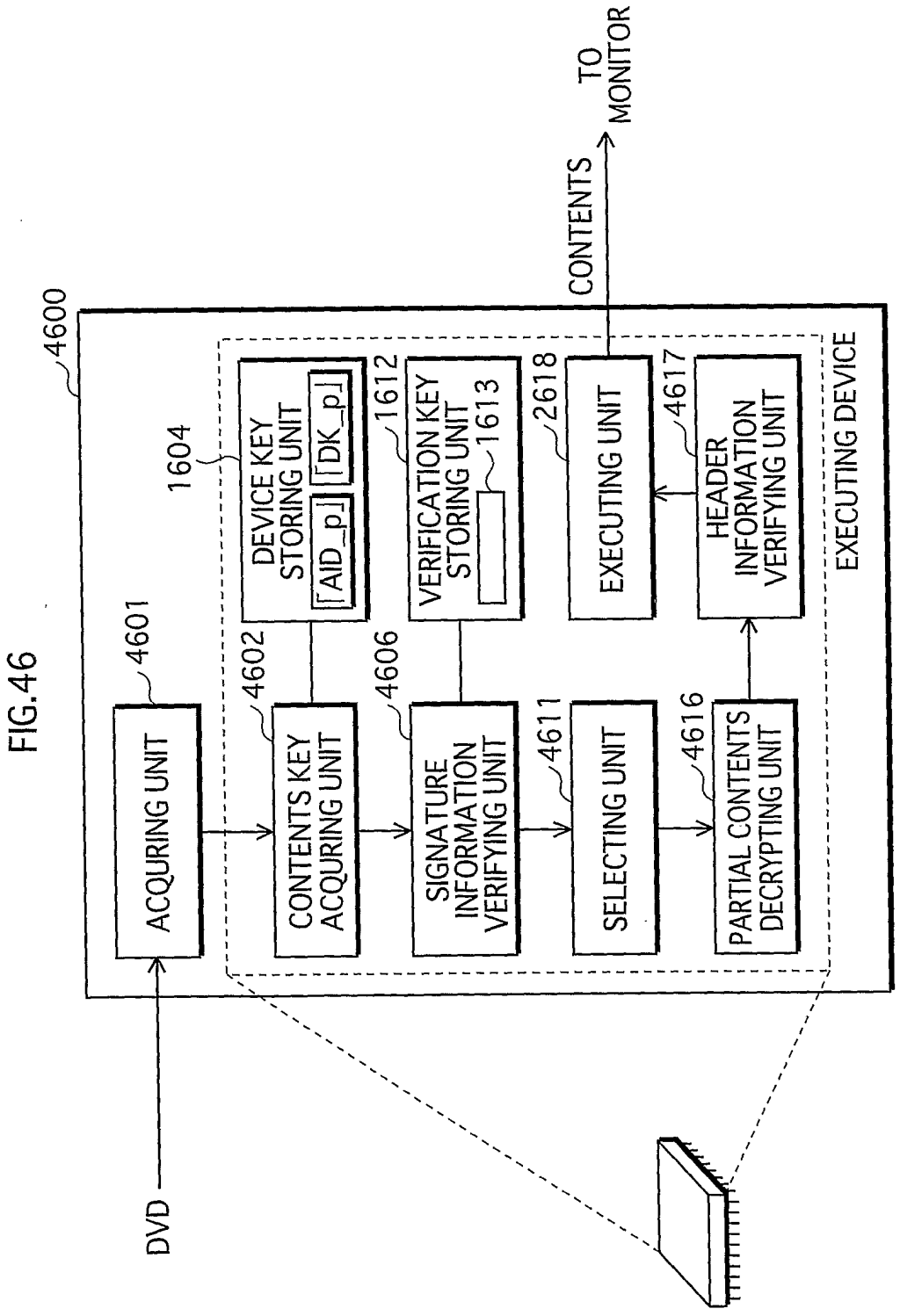

4600
EXECUTING DEVICE
4601
ACQURING UNIT
4602
CONTENTS KEY ACQURING UNIT
1604
DEVICE KEY STORING UNIT
「AID_p」
「DK_p」
1612
4606
SIGNATURE INFORMATION VERIFYING UNIT
1613
VERIFICATION KEY STORING UNIT
4611
SELECTING UNIT
2618
EXECUTING UNIT
4616
PARTIAL CONTENTS DECRYPTING UNIT
4617
HEADER INFORMATION VERIFYING UNIT
DVD
CONTENTS
TO MONITOR

FIG.47

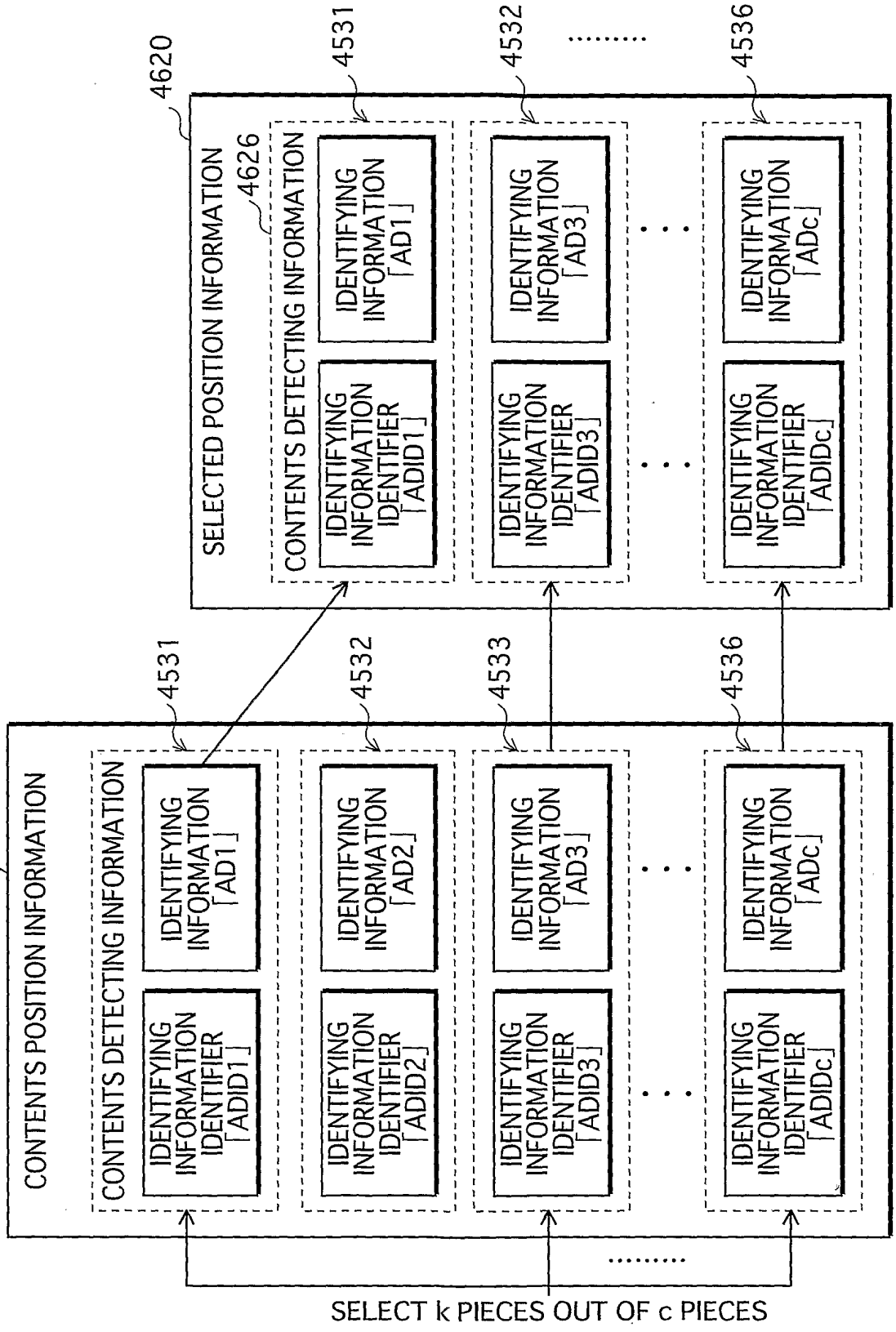

4620
4531
4532
4536
SELECTED POSITION INFORMATION
4626
CONTENTS DETECTING INFORMATION
IDENTIFYING INFORMATION [AD1]
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
IDENTIFYING INFORMATION [AD3]
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
IDENTIFYING INFORMATION [ADc]
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]
4530
4531
4532
4533
4536
CONTENTS POSITION INFORMATION
CONTENTS DETECTING INFORMATION
IDENTIFYING INFORMATION [AD1]
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
IDENTIFYING INFORMATION [AD2]
IDENTIFYING INFORMATION IDENTIFIER [ADID2]
IDENTIFYING INFORMATION [AD3]
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
IDENTIFYING INFORMATION [ADc]
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]
SELECT k PIECES OUT OF c PIECES

FIG.48

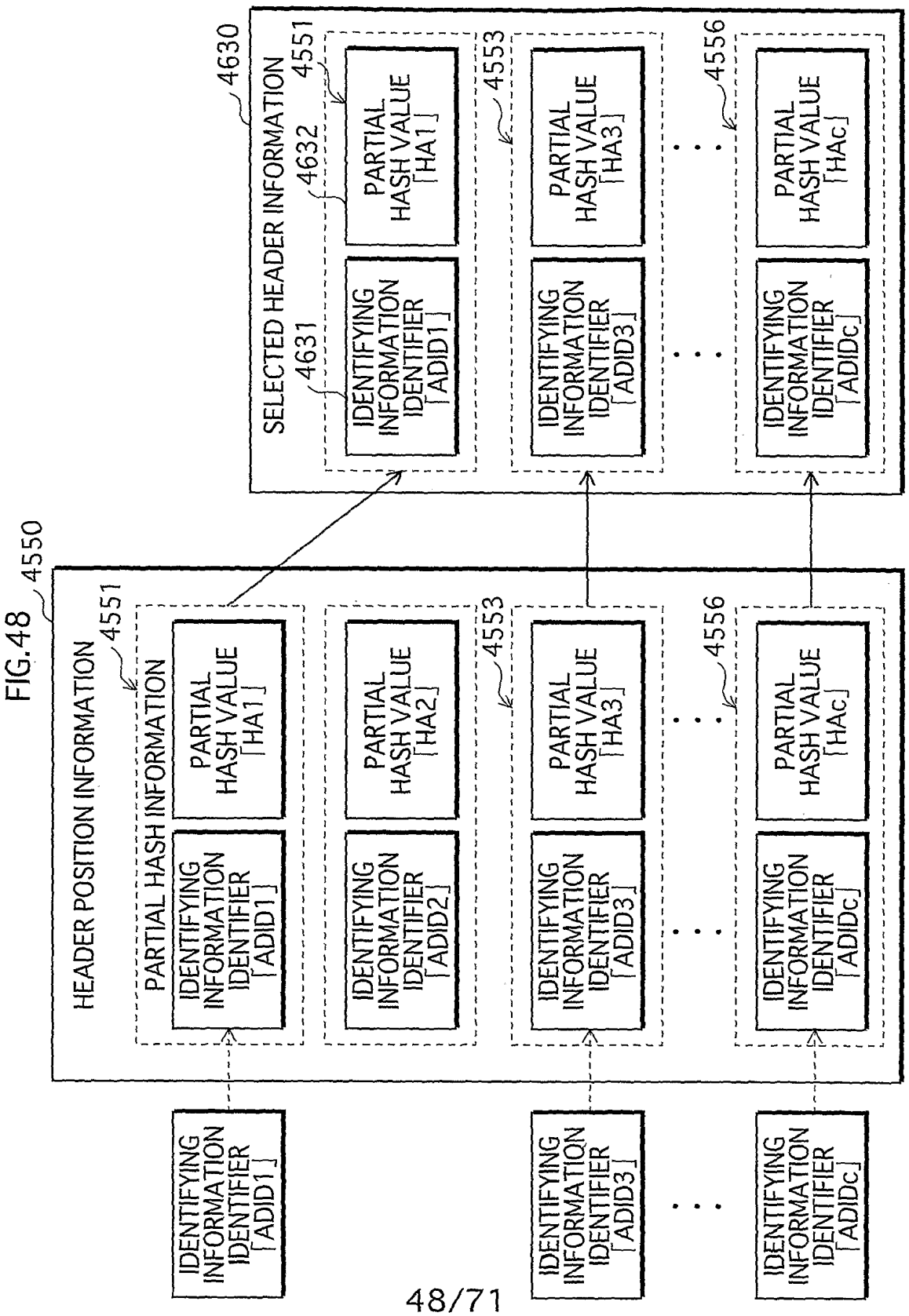

4630
SELECTED HEADER INFORMATION
4551
4632
4631
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
PARTIAL HASH VALUE [HA1]
4553
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
PARTIAL HASH VALUE [HA3]
4556
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]
PARTIAL HASH VALUE [HAc]
4550
HEADER POSITION INFORMATION
4551
PARTIAL HASH INFORMATION
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
PARTIAL HASH VALUE [HA1]
IDENTIFYING INFORMATION IDENTIFIER [ADID2]
PARTIAL HASH VALUE [HA2]
4553
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
PARTIAL HASH VALUE [HA3]
4556
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]
PARTIAL HASH VALUE [HAc]
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]

FIG.49

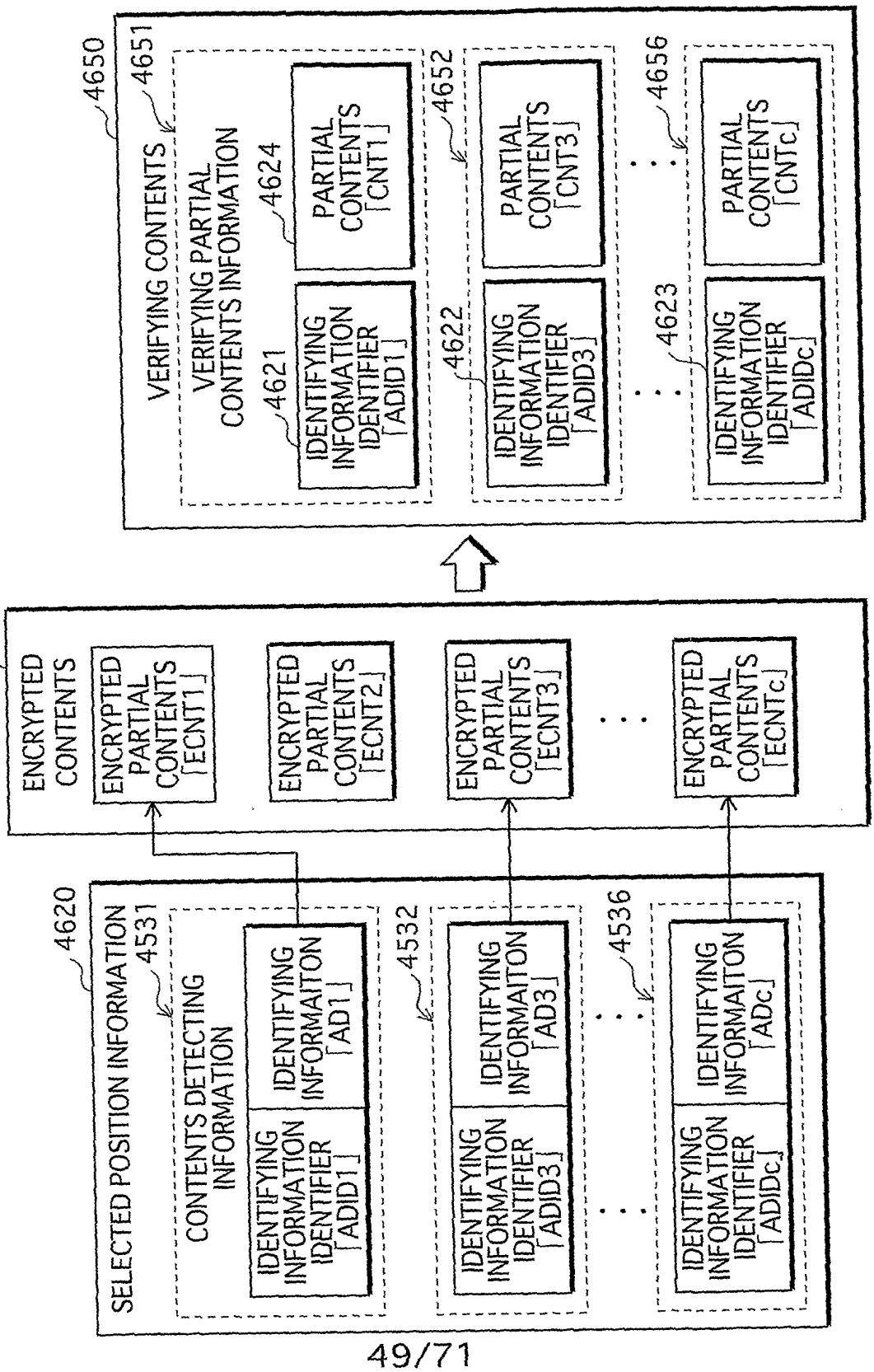

4650
4651
VERIFYING CONTENTS
VERIFYING PARTIAL CONTENTS INFORMATION
4621
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
4624
PARTIAL CONTENTS [CNT1]
4622
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
4652
PARTIAL CONTENTS [CNT3]
4623
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]
4656
PARTIAL CONTENTS [CNTc]
4580
ENCRYPTED CONTENTS
ENCRYPTED PARTIAL CONTENTS [ECNT1]
ENCRYPTED PARTIAL CONTENTS [ECNT2]
ENCRYPTED PARTIAL CONTENTS [ECNT3]
ENCRYPTED PARTIAL CONTENTS [ECNTc]
4620
SELECTED POSITION INFORMATION
4531
CONTENTS DETECTING INFORMATION
IDENTIFYING INFORMATION IDENTIFIER [ADID1]
IDENTIFYING INFORMAITON [AD1]
4532
IDENTIFYING INFORMATION IDENTIFIER [ADID3]
IDENTIFYING INFORMAITON [AD3]
4536
IDENTIFYING INFORMATION IDENTIFIER [ADIDc]
IDENTIFYING INFORMAITON [ADc]

FIG.50

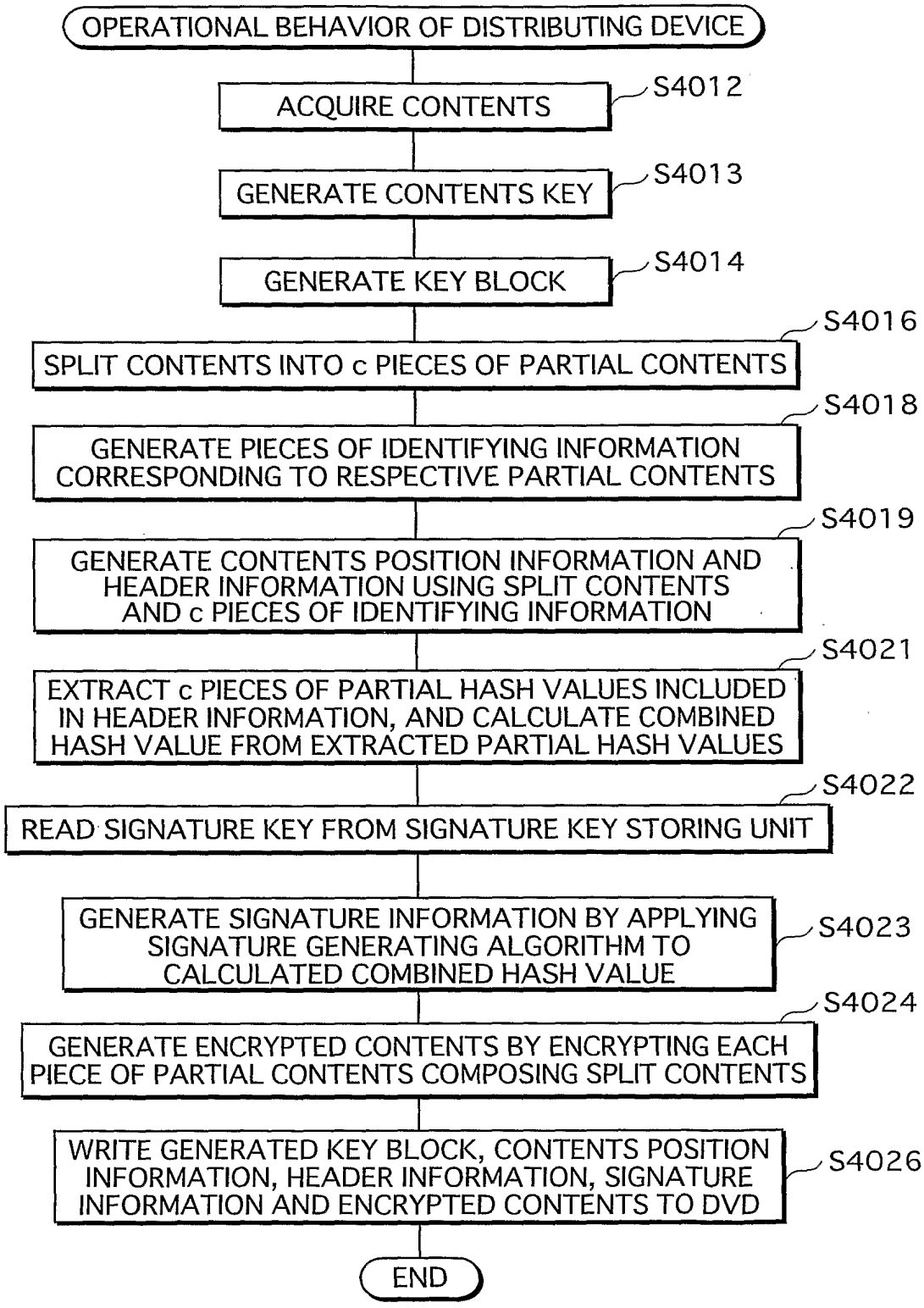

OPERATIONAL BEHAVIOR OF DISTRIBUTING DEVICE
ACQUIRE CONTENTS
S4012
GENERATE CONTENTS KEY
S4013
GENERATE KEY BLOCK
S4014
SPLIT CONTENTS INTO c PIECES OF PARTIAL CONTENTS
S4016
GENERATE PIECES OF IDENTIFYING INFORMATION CORRESPONDING TO RESPECTIVE PARTIAL CONTENTS
S4018
GENERATE CONTENTS POSITION INFORMATION AND HEADER INFORMATION USING SPLIT CONTENTS AND c PIECES OF IDENTIFYING INFORMATION
S4019
EXTRACT c PIECES OF PARTIAL HASH VALUES INCLUDED IN HEADER INFORMATION, AND CALCULATE COMBINED HASH VALUE FROM EXTRACTED PARTIAL HASH VALUES
S4021
READ SIGNATURE KEY FROM SIGNATURE KEY STORING UNIT
S4022
GENERATE SIGNATURE INFORMATION BY APPLYING SIGNATURE GENERATING ALGORITHM TO CALCULATED COMBINED HASH VALUE
S4023
GENERATE ENCRYPTED CONTENTS BY ENCRYPTING EACH PIECE OF PARTIAL CONTENTS COMPOSING SPLIT CONTENTS
S4024
WRITE GENERATED KEY BLOCK, CONTENTS POSITION INFORMATION, HEADER INFORMATION, SIGNATURE INFORMATION AND ENCRYPTED CONTENTS TO DVD
S4026
END

FIG.51

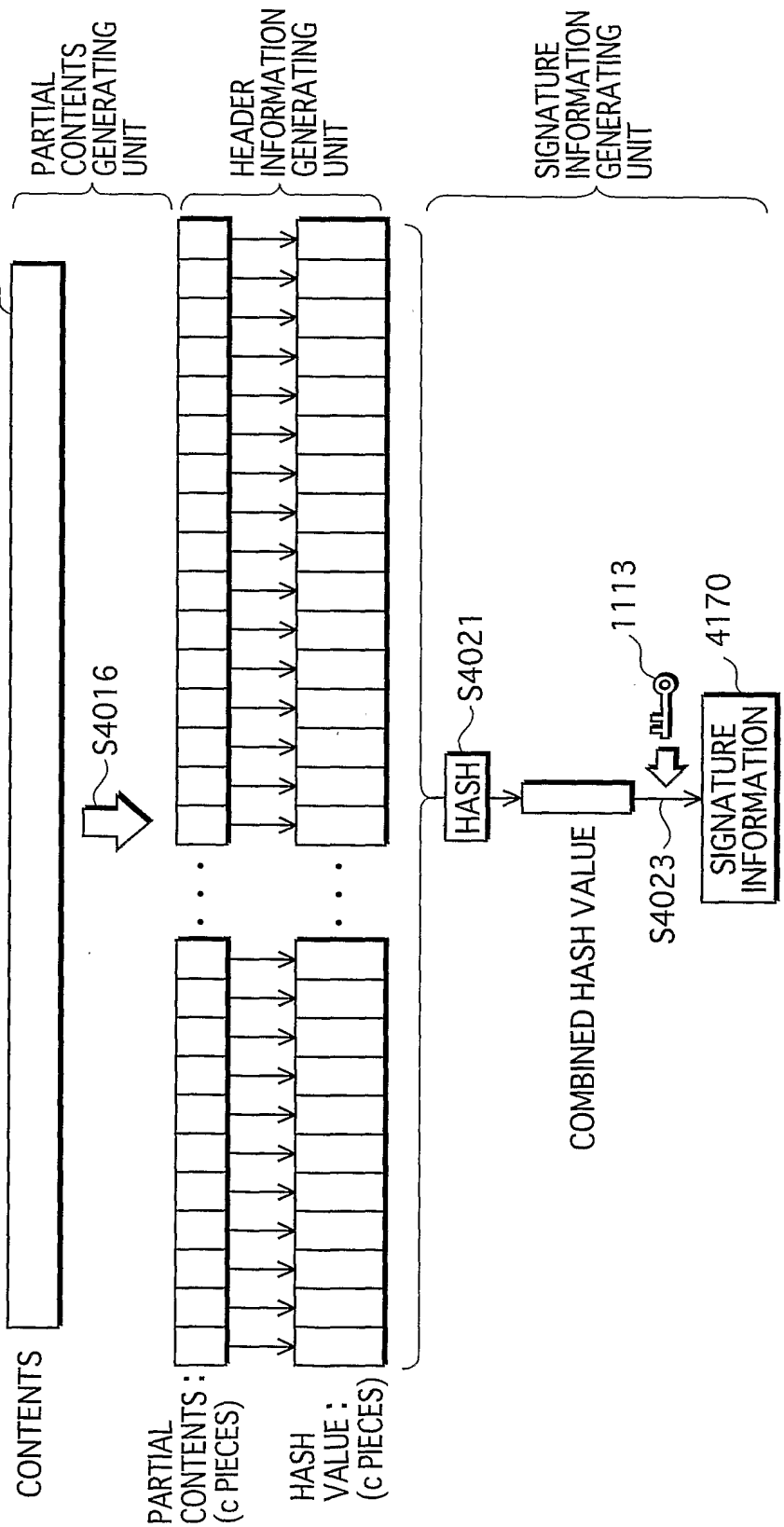

PARTIAL CONTENTS GENERATING UNIT
HEADER INFORMATION GENERATING UNIT
SIGNATURE INFORMATION GENERATING UNIT
4119
S4016
S4021
HASH
1113
4170
COMBINED HASH VALUE
S4023
SIGNATURE INFORMATION
CONTENTS
PARTIAL CONTENTS : (c PIECES)
HASH VALUE : (c PIECES)

FIG.52

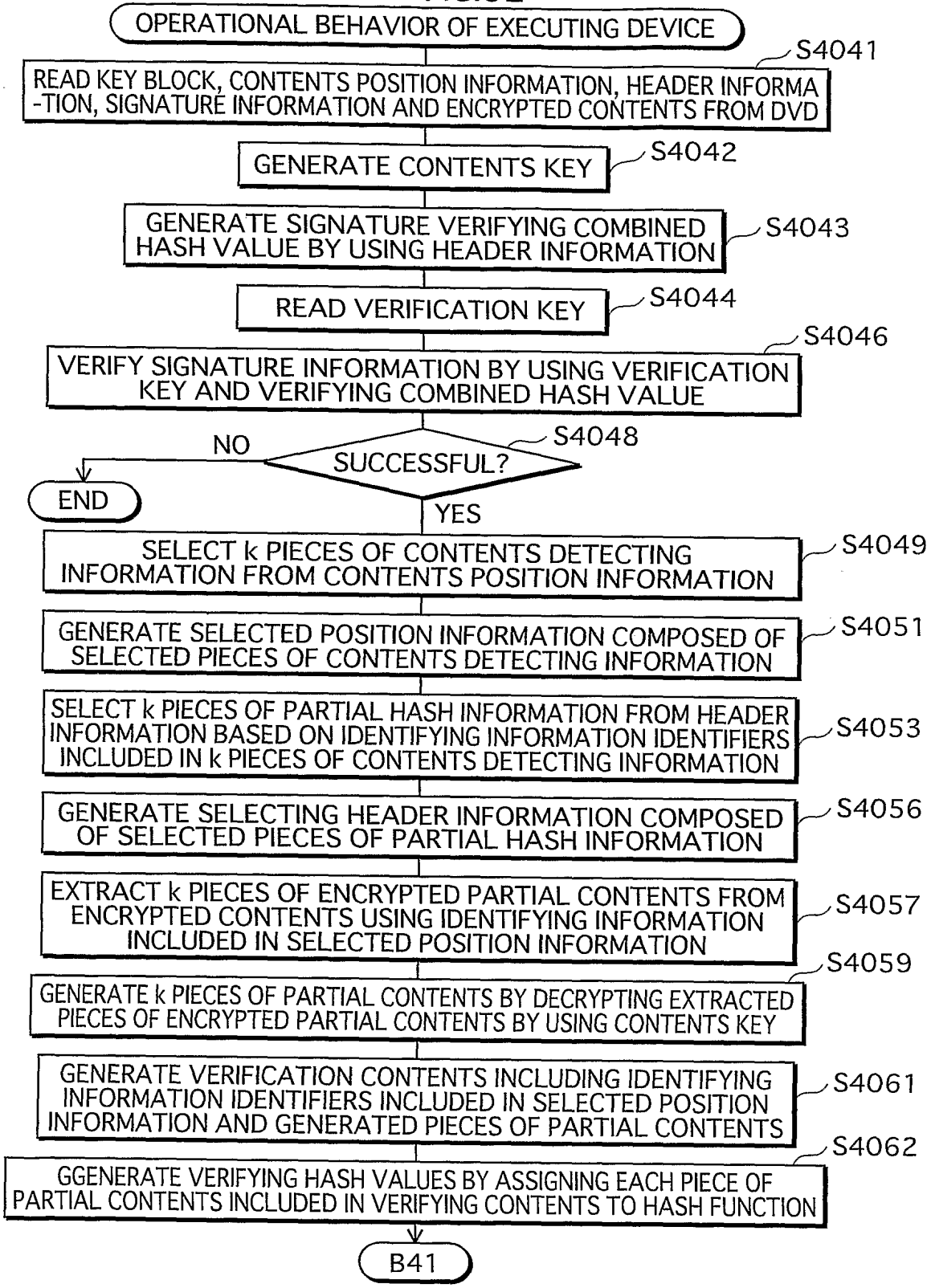

OPERATIONAL BEHAVIOR OF EXECUTING DEVICE
S4041
READ KEY BLOCK, CONTENTS POSITION INFORMATION, HEADER INFORMA -TION, SIGNATURE INFORMATION AND ENCRYPTED CONTENTS FROM DVD
GENERATE CONTENTS KEY
S4042
GENERATE SIGNATURE VERIFYING COMBINED HASH VALUE BY USING HEADER INFORMATION
S4043
READ VERIFICATION KEY
S4044
S4046
VERIFY SIGNATURE INFORMATION BY USING VERIFICATION KEY AND VERIFYING COMBINED HASH VALUE
S4048
NO
SUCCESSFUL?
END
YES
SELECT k PIECES OF CONTENTS DETECTING INFORMATION FROM CONTENTS POSITION INFORMATION
S4049
GENERATE SELECTED POSITION INFORMATION COMPOSED OF SELECTED PIECES OF CONTENTS DETECTING INFORMATION
S4051
SELECT k PIECES OF PARTIAL HASH INFORMATION FROM HEADER INFORMATION BASED ON IDENTIFYING INFORMATION IDENTIFIERS INCLUDED IN k PIECES OF CONTENTS DETECTING INFORMATION
S4053
GENERATE SELECTING HEADER INFORMATION COMPOSED OF SELECTED PIECES OF PARTIAL HASH INFORMATION
S4056
EXTRACT k PIECES OF ENCRYPTED PARTIAL CONTENTS FROM ENCRYPTED CONTENTS USING IDENTIFYING INFORMATION INCLUDED IN SELECTED POSITION INFORMATION
S4057
S4059
GENERATE k PIECES OF PARTIAL CONTENTS BY DECRYPTING EXTRACTED PIECES OF ENCRYPTED PARTIAL CONTENTS BY USING CONTENTS KEY
GENERATE VERIFICATION CONTENTS INCLUDING IDENTIFYING INFORMATION IDENTIFIERS INCLUDED IN SELECTED POSITION INFORMATION AND GENERATED PIECES OF PARTIAL CONTENTS
S4061
S4062
GGENERATE VERIFYING HASH VALUES BY ASSIGNING EACH PIECE OF PARTIAL CONTENTS INCLUDED IN VERIFYING CONTENTS TO HASH FUNCTION
B41

FIG.53

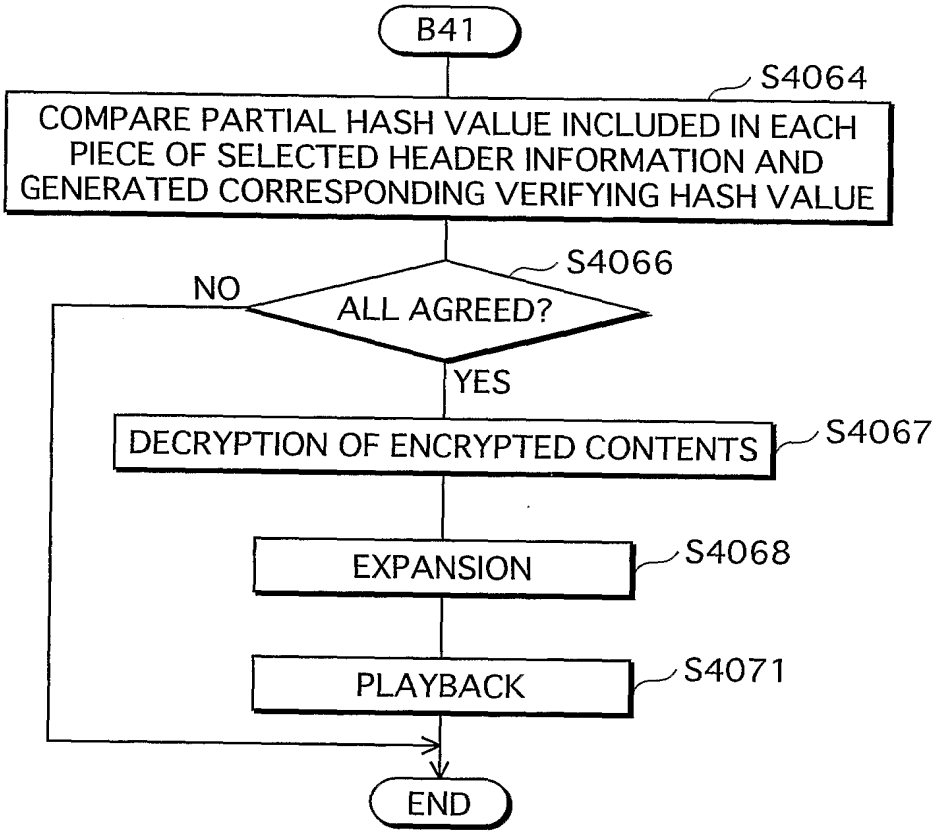

B41
S4064
COMPARE PARTIAL HASH VALUE INCLUDED IN EACH PIECE OF SELECTED HEADER INFORMATION AND GENERATED CORRESPONDING VERIFYING HASH VALUE
S4066
NO
ALL AGREED?
YES
DECRYPTION OF ENCRYPTED CONTENTS
S4067
EXPANSION
S4068
PLAYBACK
S4071
END

FIG.54

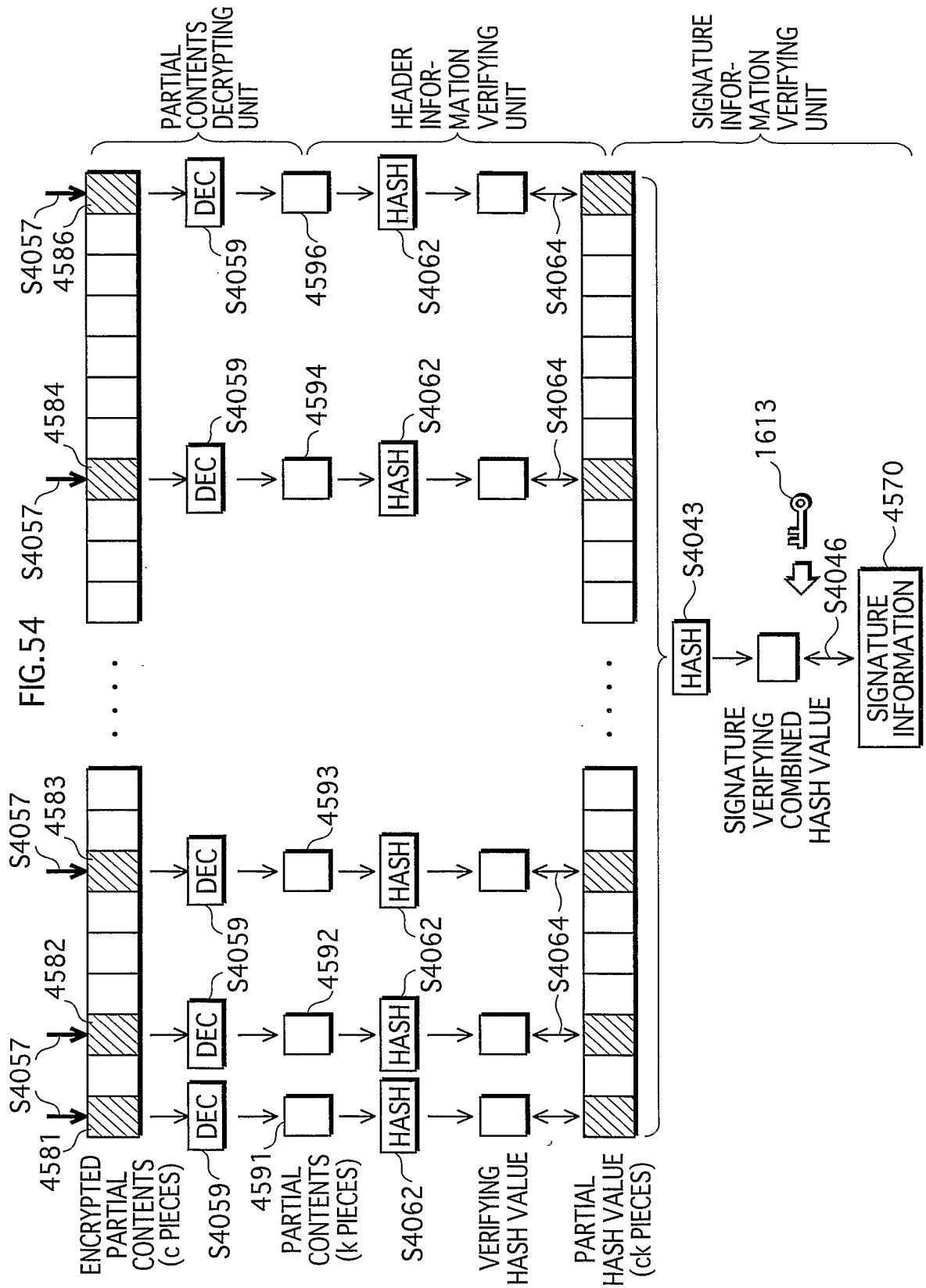

PARTIAL CONTENTS DECRYPTING UNIT
HEADER INFOR-MATION VERIFYING UNIT
SIGNATURE INFOR-MATION VERIFYING UNIT
S4057
4581
4582
4583
4584
4586
DEC
S4059
4591
4592
4593
4594
4596
HASH
S4062
S4064
S4043
S4046
1613
4570
ENCRYPTED PARTIAL CONTENTS (c PIECES)
PARTIAL CONTENTS (k PIECES)
VERIFYING HASH VALUE
PARTIAL HASH VALUE (ck PIECES)
SIGNATURE VERIFYING COMBINED HASH VALUE
SIGNATURE INFORMATION

FIG.55

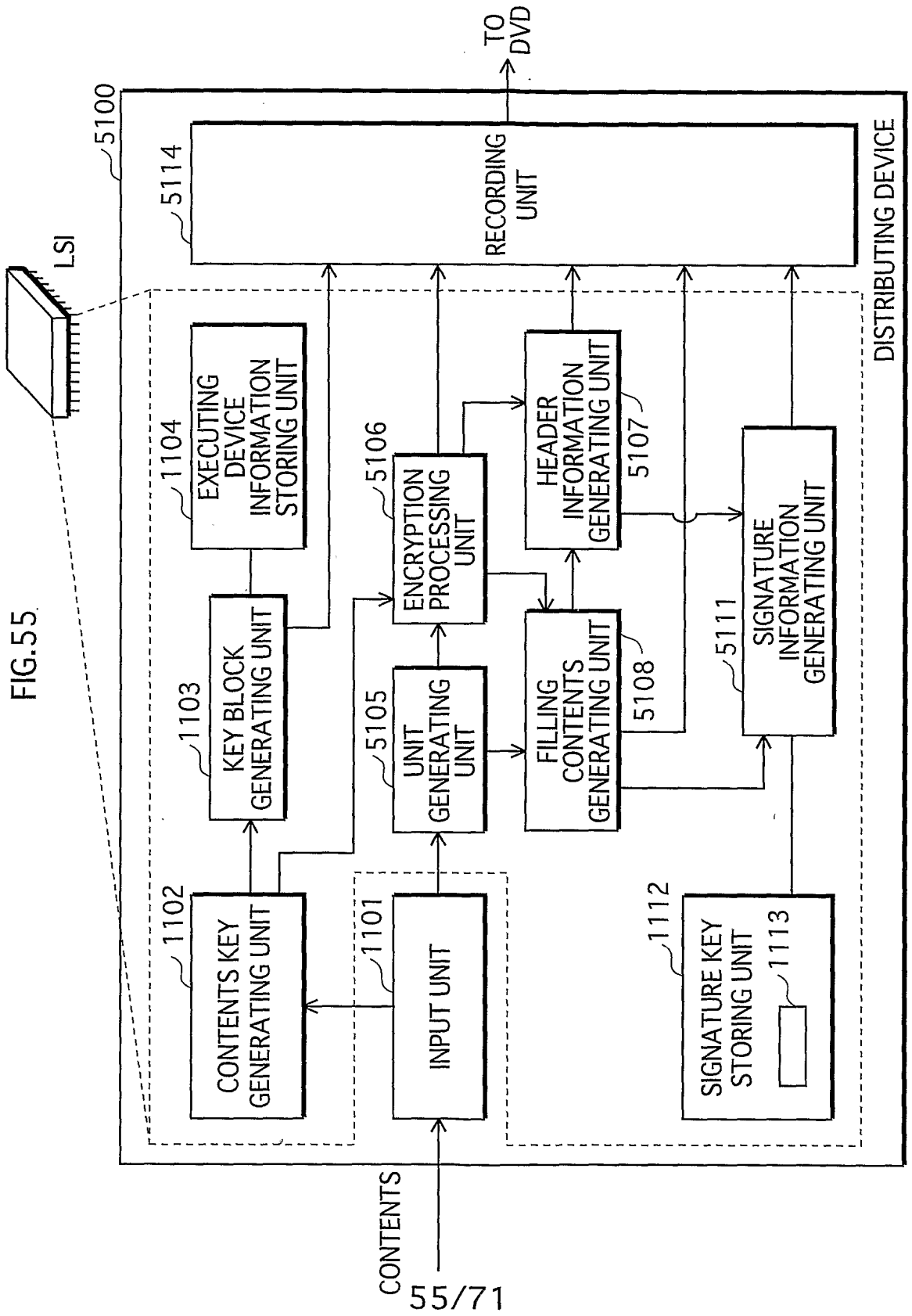

LSI
5100
DISTRIBUTING DEVICE
TO DVD
5114
RECORDING UNIT
1104
EXECUTING DEVICE INFORMATION STORING UNIT
5106
ENCRYPTION PROCESSING UNIT
HEADER INFORMATION GENERATING UNIT
5107
1103
KEY BLOCK GENERATING UNIT
5105
UNIT GENERATING UNIT
FILLING CONTENTS GENERATING UNIT
5108
5111
SIGNATURE INFORMATION GENERATING UNIT
1102
CONTENTS KEY GENERATING UNIT
1101
INPUT UNIT
1112
SIGNATURE KEY STORING UNIT
1113
CONTENTS

FIG.56

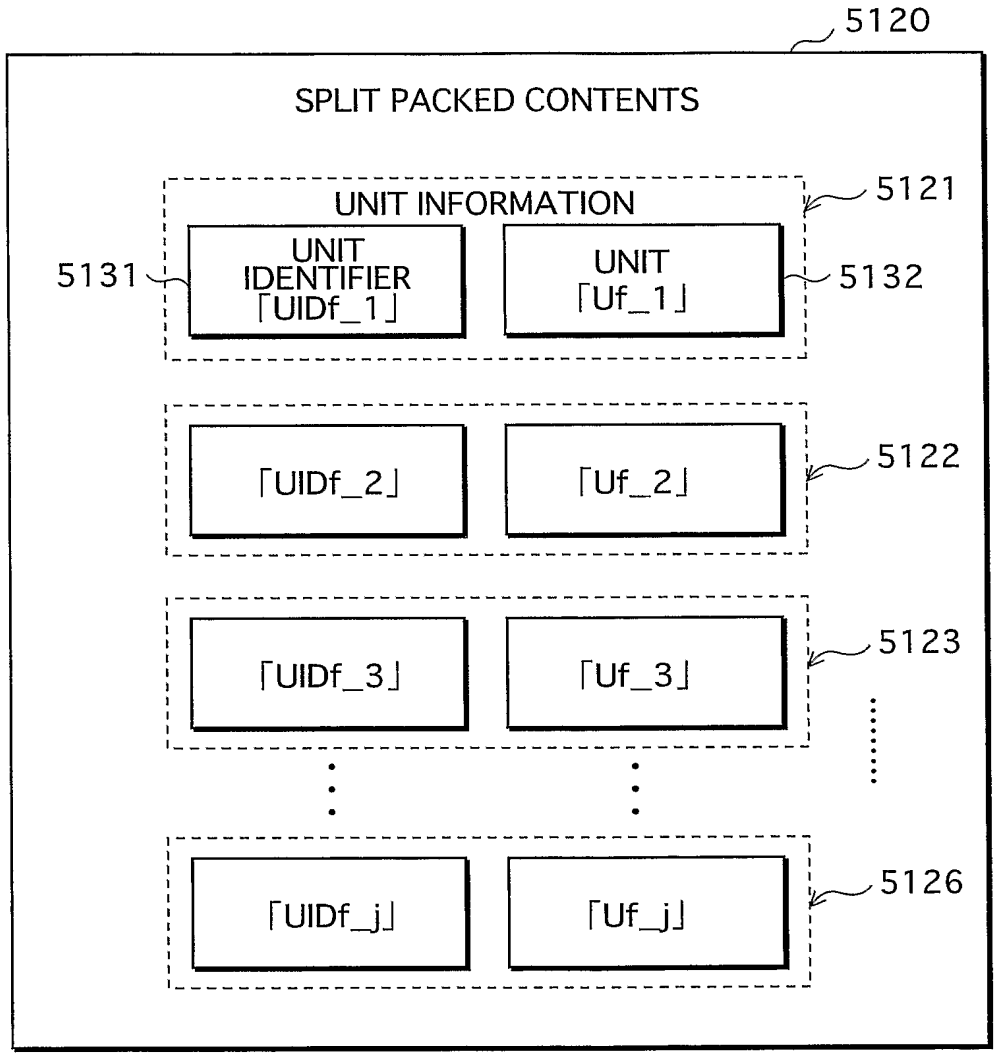

5120
SPLIT PACKED CONTENTS
UNIT INFORMATION
5121
5131
UNIT IDENTIFIER 「UIDf_1」
UNIT 「Uf_1」
5132
「UIDf_2」
「Uf_2」
5122
「UIDf_3」
「Uf_3」
5123
「UIDf_j」
「Uf_j」
5126

FIG.57

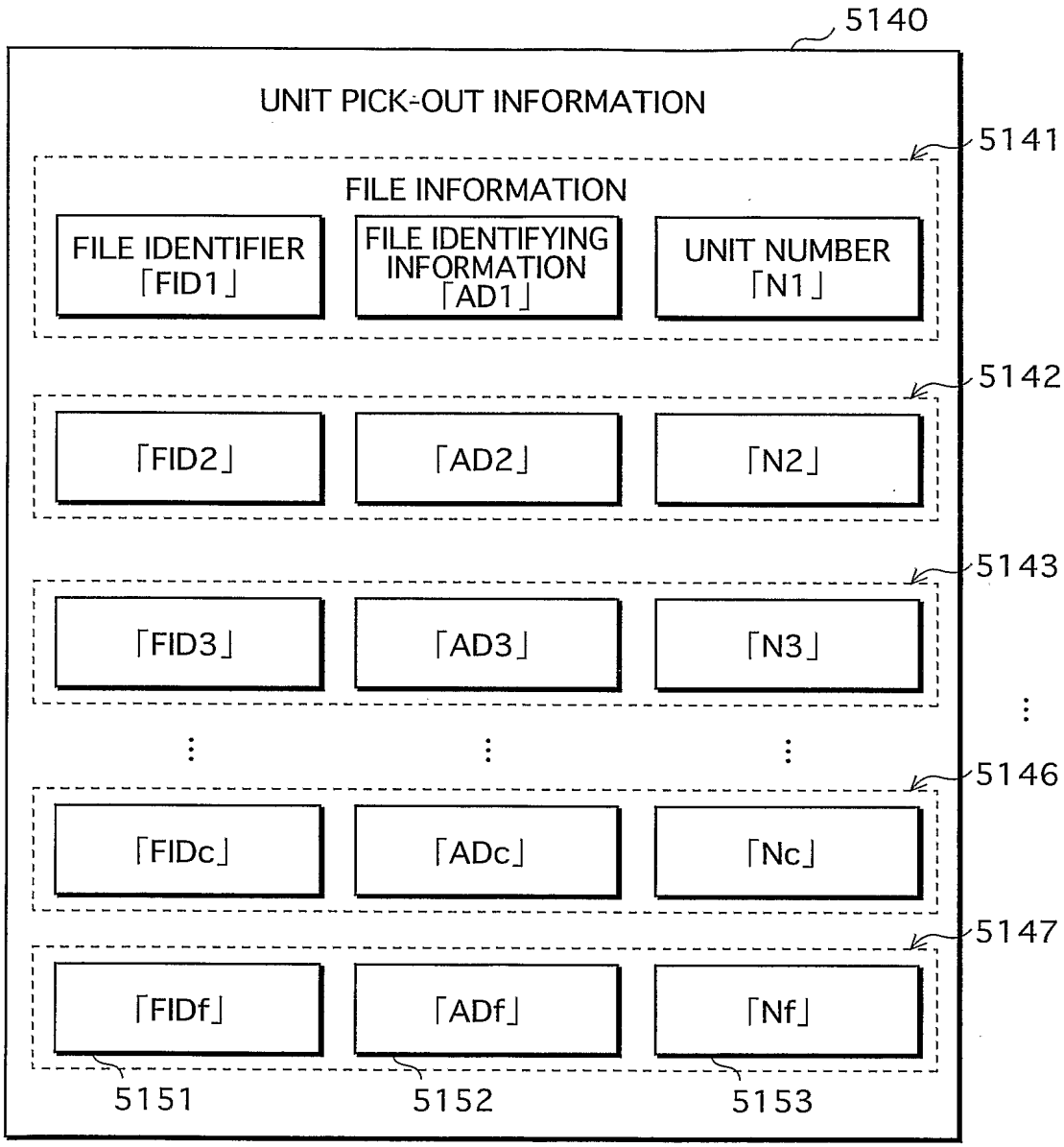

5140
UNIT PICK-OUT INFORMATION
5141
FILE INFORMATION
FILE IDENTIFIER 「FID1」
FILE IDENTIFYING INFORMATION 「AD1」
UNIT NUMBER 「N1」
5142
「FID2」
「AD2」
「N2」
5143
「FID3」
「AD3」
「N3」
5146
「FIDc」
「ADc」
「Nc」
5147
「FIDf」
「ADf」
「Nf」
5151
5152
5153

FIG.58

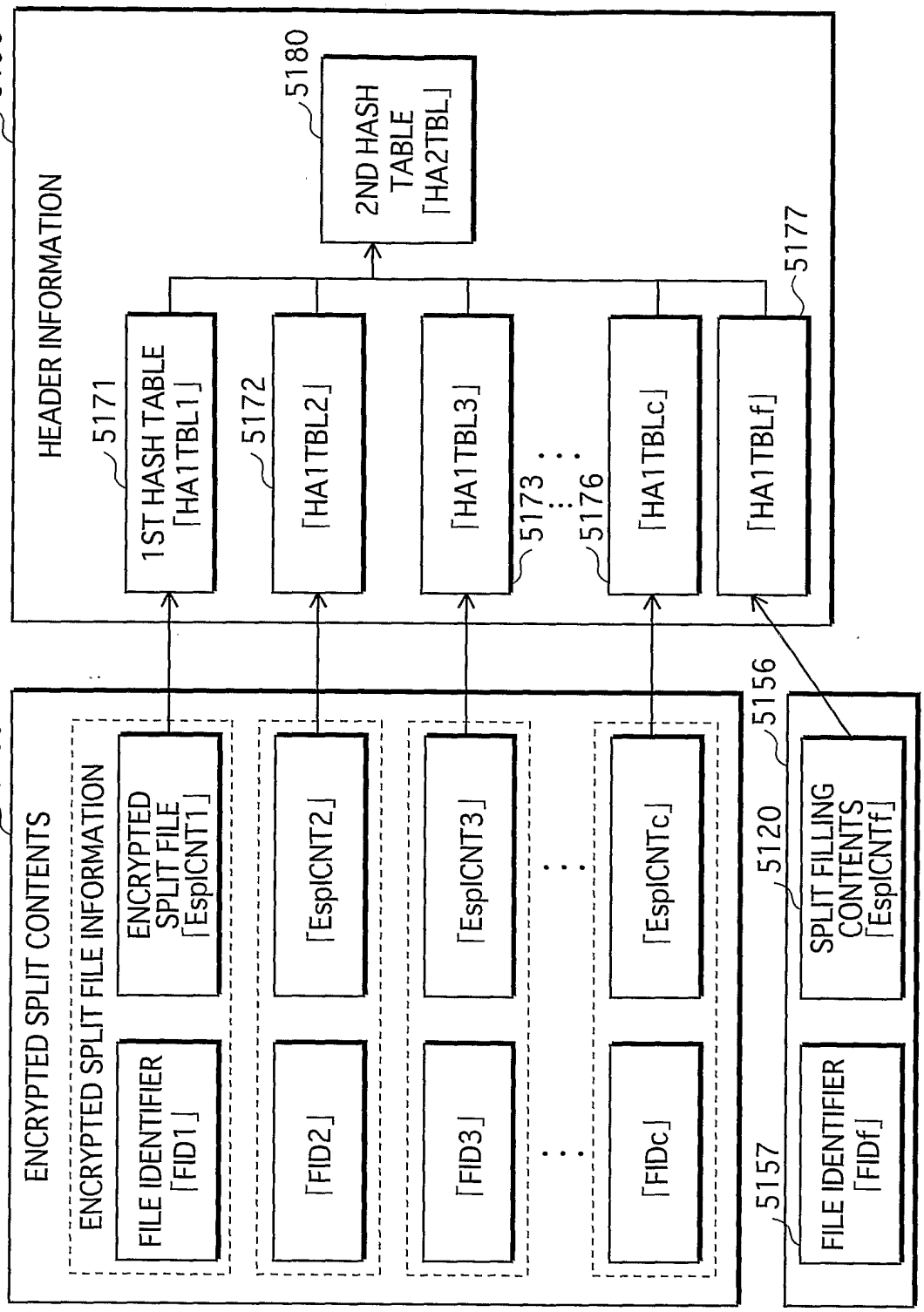

5190
HEADER INFORMATION
5180
2ND HASH TABLE 「HA2TBL」
5171
1ST HASH TABLE 「HA1TBL1」
5172
「HA1TBL2」
「HA1TBL3」
5173
5176
「HA1TBLc」
「HA1TBLf」
5177
5160
ENCRYPTED SPLIT CONTENTS
ENCRYPTED SPLIT FILE INFORMATION
FILE IDENTIFIER 「FID1」
ENCRYPTED SPLIT FILE 「EsplCNT1」
「FID2」
「EsplCNT2」
「FID3」
「EsplCNT3」
「FIDc」
「EsplCNTc」
5156
5120
SPLIT FILLING CONTENTS 「EsplCNTf」
5157
FILE IDENTIFIER 「FIDf」

FIG.59

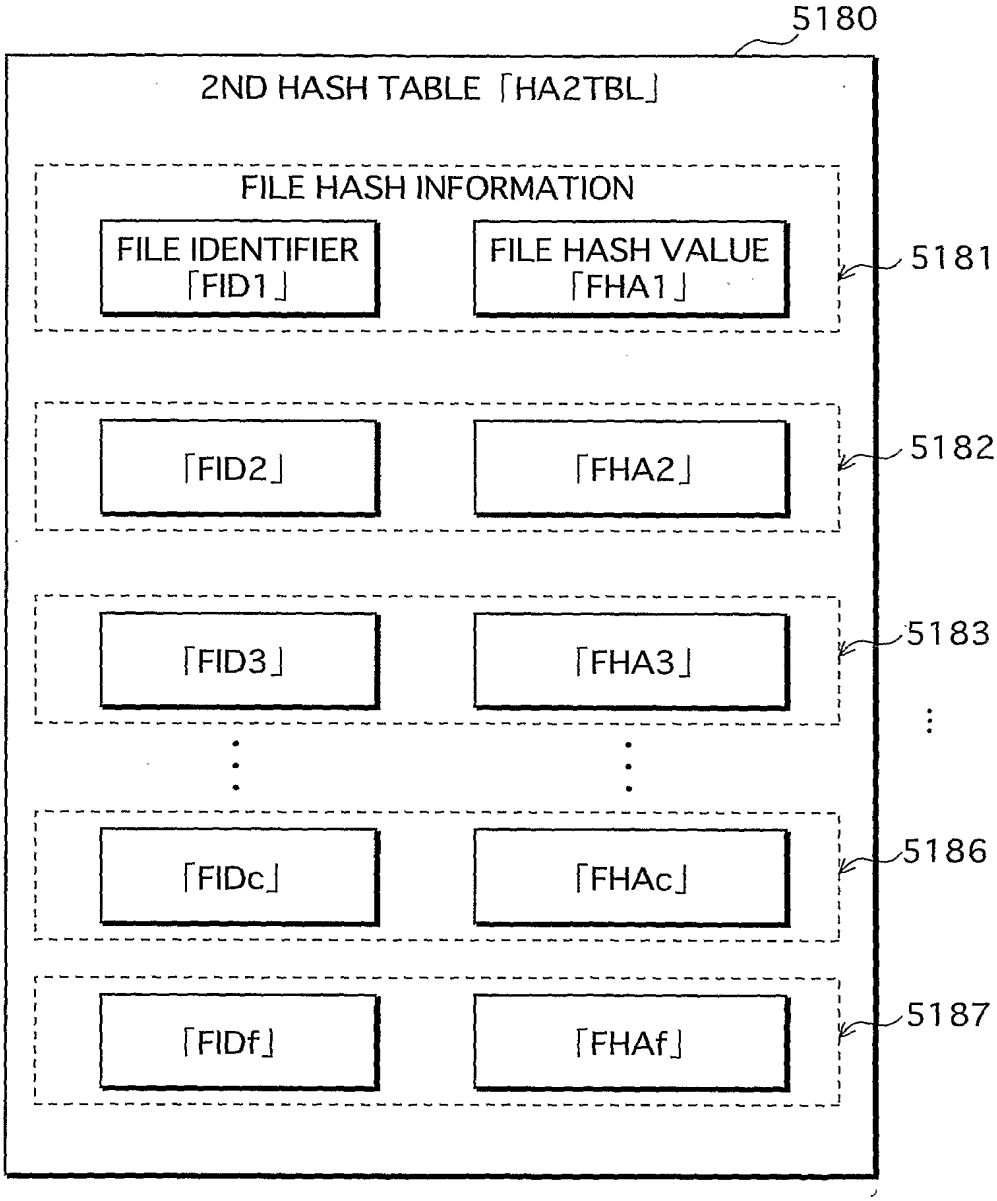

5180
2ND HASH TABLE「HA2TBL」
FILE HASH INFORMATION
FILE IDENTIFIER「FID1」
FILE HASH VALUE「FHA1」
5181
「FID2」
「FHA2」
5182
「FID3」
「FHA3」
5183
「FIDc」
「FHAc」
5186
「FIDf」
「FHAf」
5187

FIG.60

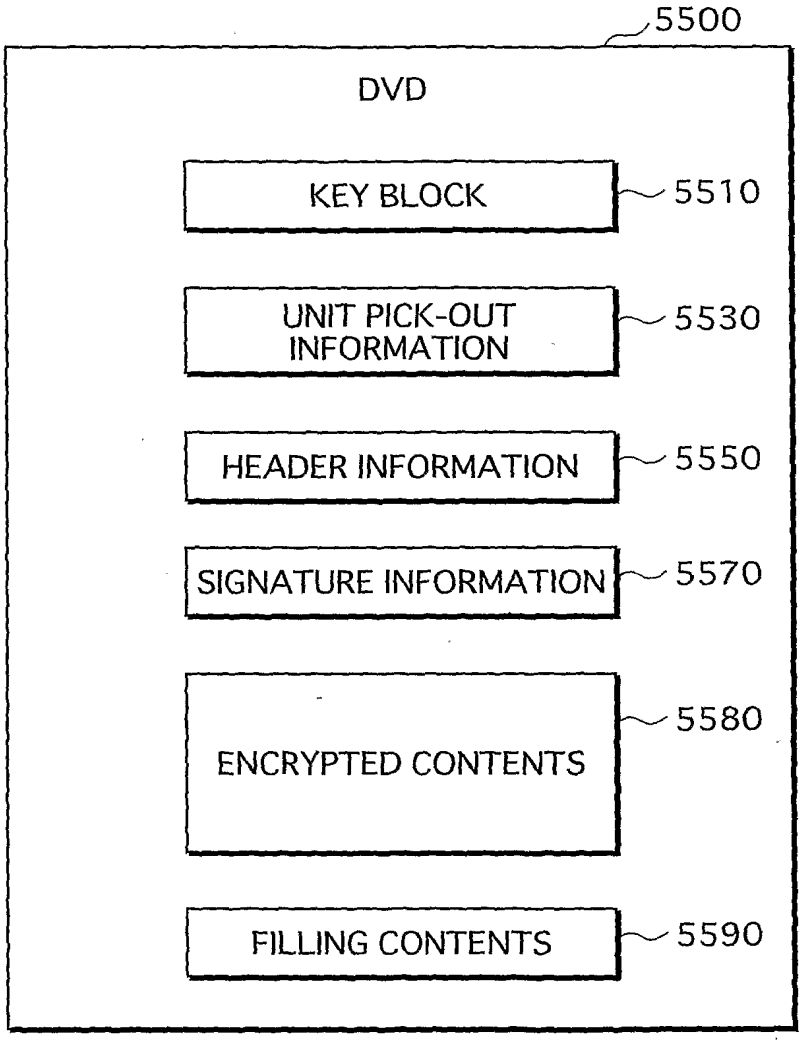

5500
DVD
KEY BLOCK
5510
UNIT PICK-OUT INFORMATION
5530
HEADER INFORMATION
5550
SIGNATURE INFORMATION
5570
ENCRYPTED CONTENTS
5580
FILLING CONTENTS
5590

FIG.61

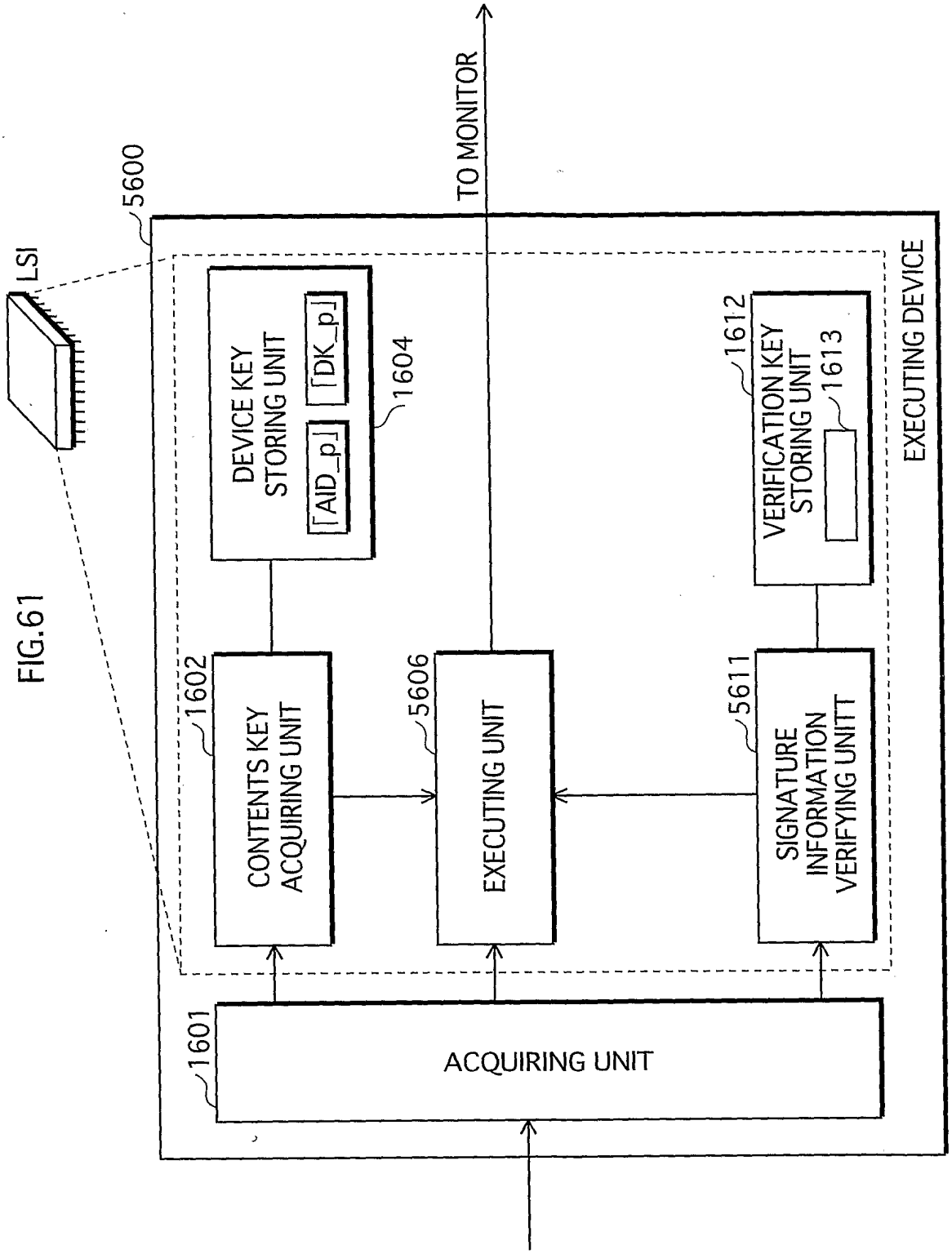

LSI
5600
TO MONITOR
EXECUTING DEVICE
DEVICE KEY STORING UNIT
「AID_p」
「DK_p」
1604
1612
VERIFICATION KEY STORING UNIT
1613
1602
CONTENTS KEY ACQUIRING UNIT
5606
EXECUTING UNIT
5611
SIGNATURE INFORMATION VERIFYING UNITT
1601
ACQUIRING UNIT

FIG.62

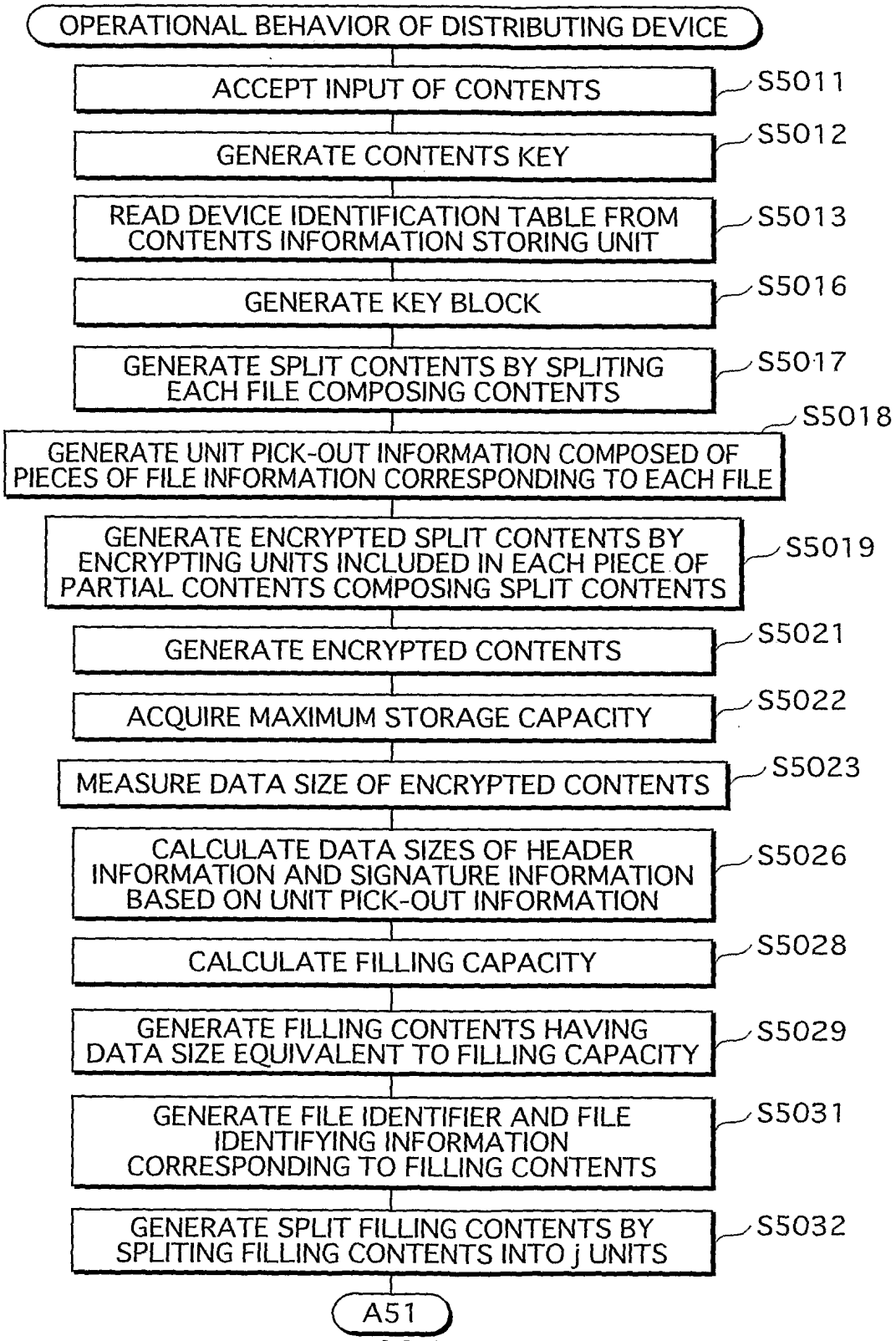

OPERATIONAL BEHAVIOR OF DISTRIBUTING DEVICE
ACCEPT INPUT OF CONTENTS
S5011
GENERATE CONTENTS KEY
S5012
READ DEVICE IDENTIFICATION TABLE FROM CONTENTS INFORMATION STORING UNIT
S5013
GENERATE KEY BLOCK
S5016
GENERATE SPLIT CONTENTS BY SPLITING EACH FILE COMPOSING CONTENTS
S5017
GENERATE UNIT PICK-OUT INFORMATION COMPOSED OF PIECES OF FILE INFORMATION CORRESPONDING TO EACH FILE
S5018
GENERATE ENCRYPTED SPLIT CONTENTS BY ENCRYPTING UNITS INCLUDED IN EACH PIECE OF PARTIAL CONTENTS COMPOSING SPLIT CONTENTS
S5019
GENERATE ENCRYPTED CONTENTS
S5021
ACQUIRE MAXIMUM STORAGE CAPACITY
S5022
MEASURE DATA SIZE OF ENCRYPTED CONTENTS
S5023
CALCULATE DATA SIZES OF HEADER INFORMATION AND SIGNATURE INFORMATION BASED ON UNIT PICK-OUT INFORMATION
S5026
CALCULATE FILLING CAPACITY
S5028
GENERATE FILLING CONTENTS HAVING DATA SIZE EQUIVALENT TO FILLING CAPACITY
S5029
GENERATE FILE IDENTIFIER AND FILE IDENTIFYING INFORMATION CORRESPONDING TO FILLING CONTENTS
S5031
GENERATE SPLIT FILLING CONTENTS BY SPLITING FILLING CONTENTS INTO j UNITS
S5032
A51

FIG.63

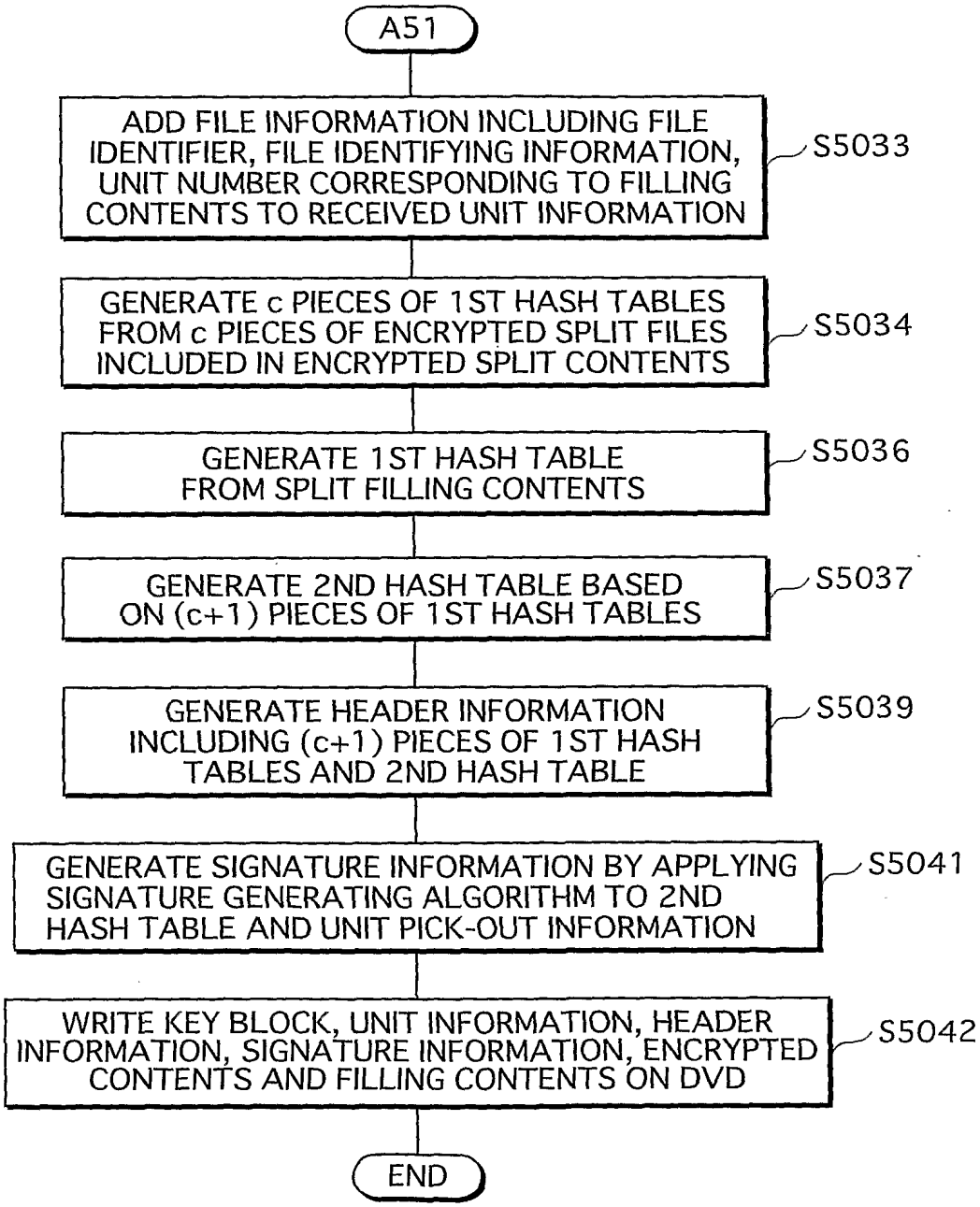

A51
ADD FILE INFORMATION INCLUDING FILE IDENTIFIER, FILE IDENTIFYING INFORMATION, UNIT NUMBER CORRESPONDING TO FILLING CONTENTS TO RECEIVED UNIT INFORMATION
S5033
GENERATE c PIECES OF 1ST HASH TABLES FROM c PIECES OF ENCRYPTED SPLIT FILES INCLUDED IN ENCRYPTED SPLIT CONTENTS
S5034
GENERATE 1ST HASH TABLE FROM SPLIT FILLING CONTENTS
S5036
GENERATE 2ND HASH TABLE BASED ON (c+1) PIECES OF 1ST HASH TABLES
S5037
GENERATE HEADER INFORMATION INCLUDING (c+1) PIECES OF 1ST HASH TABLES AND 2ND HASH TABLE
S5039
GENERATE SIGNATURE INFORMATION BY APPLYING SIGNATURE GENERATING ALGORITHM TO 2ND HASH TABLE AND UNIT PICK-OUT INFORMATION
S5041
WRITE KEY BLOCK, UNIT INFORMATION, HEADER INFORMATION, SIGNATURE INFORMATION, ENCRYPTED CONTENTS AND FILLING CONTENTS ON DVD
S5042
END

FIG.64

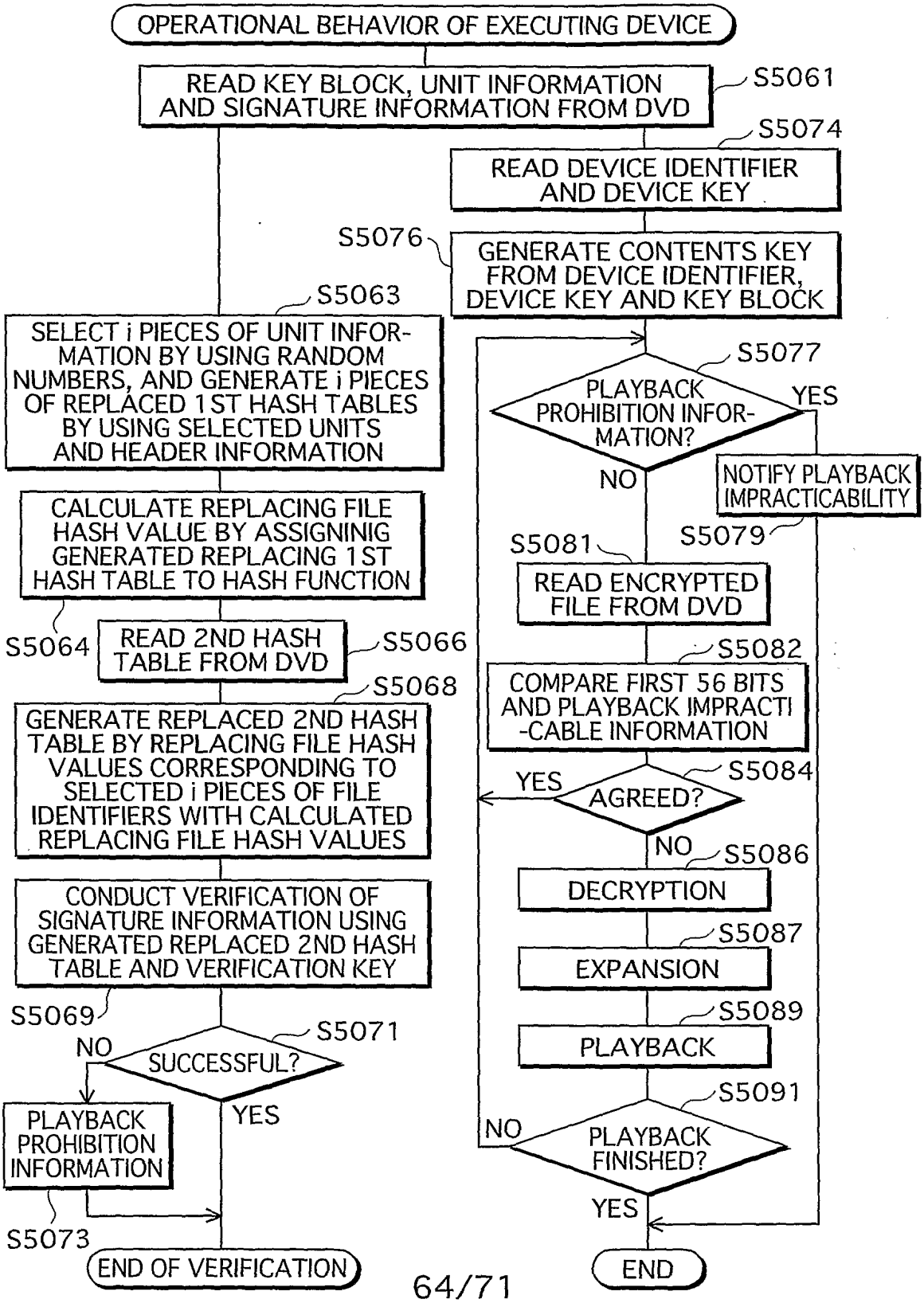

OPERATIONAL BEHAVIOR OF EXECUTING DEVICE
READ KEY BLOCK, UNIT INFORMATION AND SIGNATURE INFORMATION FROM DVD
S5061
READ DEVICE IDENTIFIER AND DEVICE KEY
S5074
GENERATE CONTENTS KEY FROM DEVICE IDENTIFIER, DEVICE KEY AND KEY BLOCK
S5076
SELECT i PIECES OF UNIT INFORMATION BY USING RANDOM NUMBERS, AND GENERATE i PIECES OF REPLACED 1ST HASH TABLES BY USING SELECTED UNITS AND HEADER INFORMATION
S5063
CALCULATE REPLACING FILE HASH VALUE BY ASSIGNINIG GENERATED REPLACING 1ST HASH TABLE TO HASH FUNCTION
S5064
READ 2ND HASH TABLE FROM DVD
S5066
GENERATE REPLACED 2ND HASH TABLE BY REPLACING FILE HASH VALUES CORRESPONDING TO SELECTED i PIECES OF FILE IDENTIFIERS WITH CALCULATED REPLACING FILE HASH VALUES
S5068
CONDUCT VERIFICATION OF SIGNATURE INFORMATION USING GENERATED REPLACED 2ND HASH TABLE AND VERIFICATION KEY
S5069
SUCCESSFUL?
S5071
NO
YES
PLAYBACK PROHIBITION INFORMATION
S5073
END OF VERIFICATION
PLAYBACK PROHIBITION INFORMATION?
S5077
YES
NO
NOTIFY PLAYBACK IMPRACTICABILITY
S5079
READ ENCRYPTED FILE FROM DVD
S5081
COMPARE FIRST 56 BITS AND PLAYBACK IMPRACTI-CABLE INFORMATION
S5082
AGREED?
S5084
YES
NO
DECRYPTION
S5086
EXPANSION
S5087
PLAYBACK
S5089
PLAYBACK FINISHED?
S5091
NO
YES
END

FIG.65

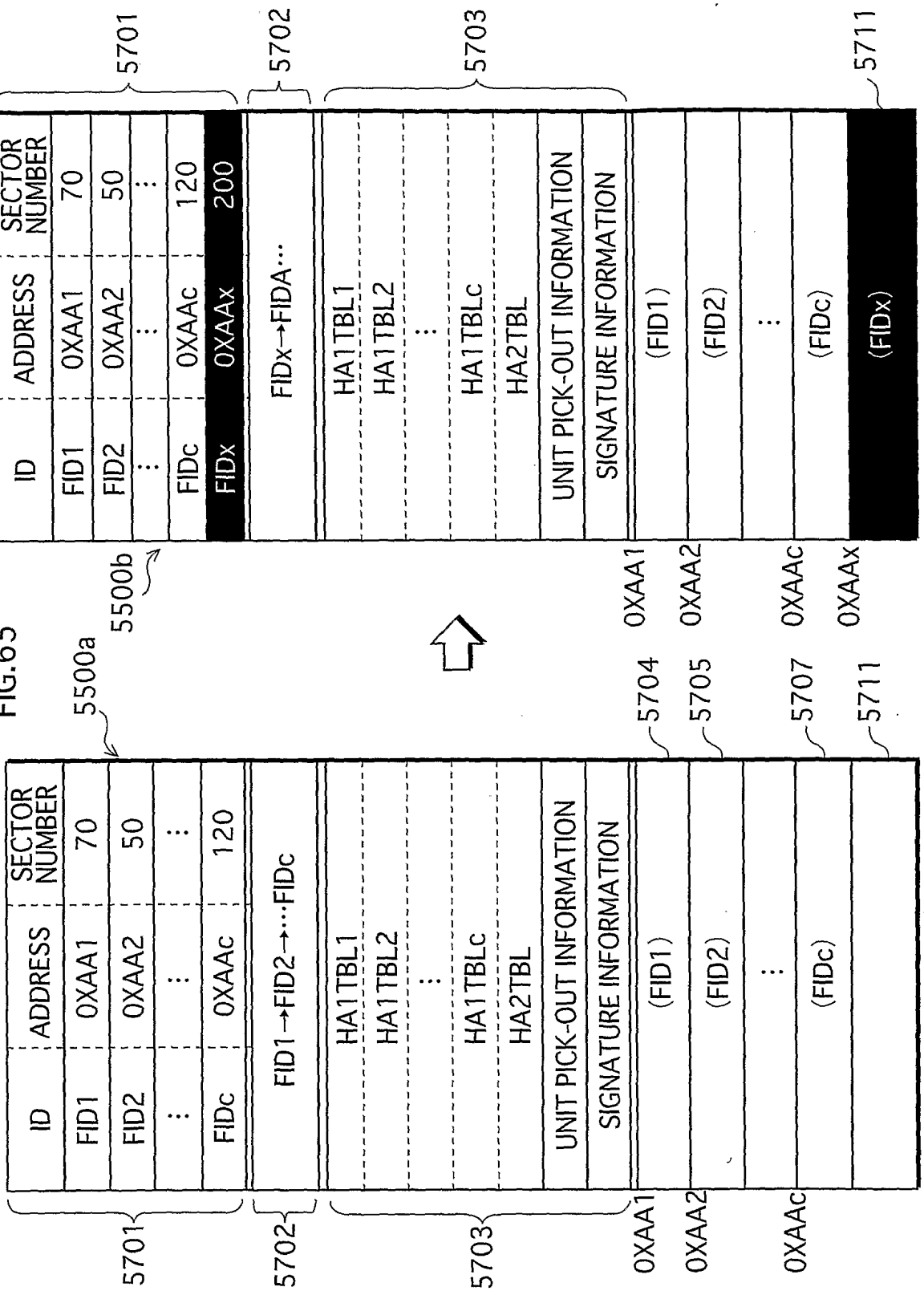

5500a
5500b
5701
5702
5703
5704
5705
5707
5711
ID
ADDRESS
SECTOR NUMBER
FID1
0XAA1
70
FID2
0XAA2
50
FIDc
0XAAc
120
FIDx
0XAAx
200
FID1→FID2→…FIDc
FIDx→FIDA…
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
UNIT PICK-OUT INFORMATION
SIGNATURE INFORMATION
(FID1)
(FID2)
(FIDc)
(FIDx)
0XAA1
0XAA2
0XAAc
0XAAx

FIG.66

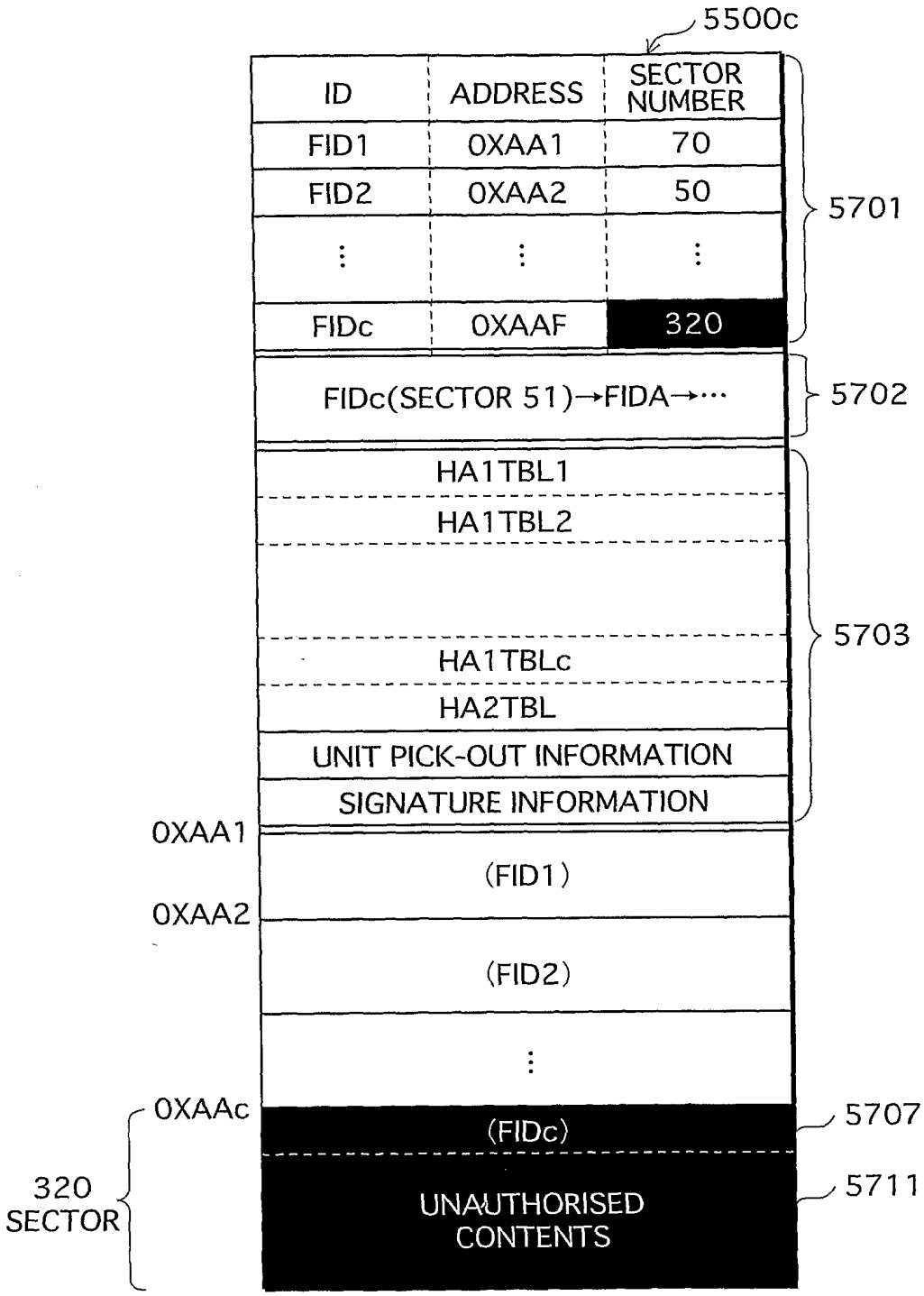

5500c
ID
ADDRESS
SECTOR NUMBER
FID1
0XAA1
70
FID2
0XAA2
50
FIDc
0XAAF
320
5701
FIDc(SECTOR 51)→FIDA→…
5702
HA1TBL1
HA1TBL2
HA1TBLc
HA2TBL
UNIT PICK-OUT INFORMATION
SIGNATURE INFORMATION
5703
0XAA1
(FID1)
0XAA2
(FID2)
0XAAc
(FIDc)
5707
320 SECTOR
UNAUTHORISED CONTENTS
5711

FIG.67

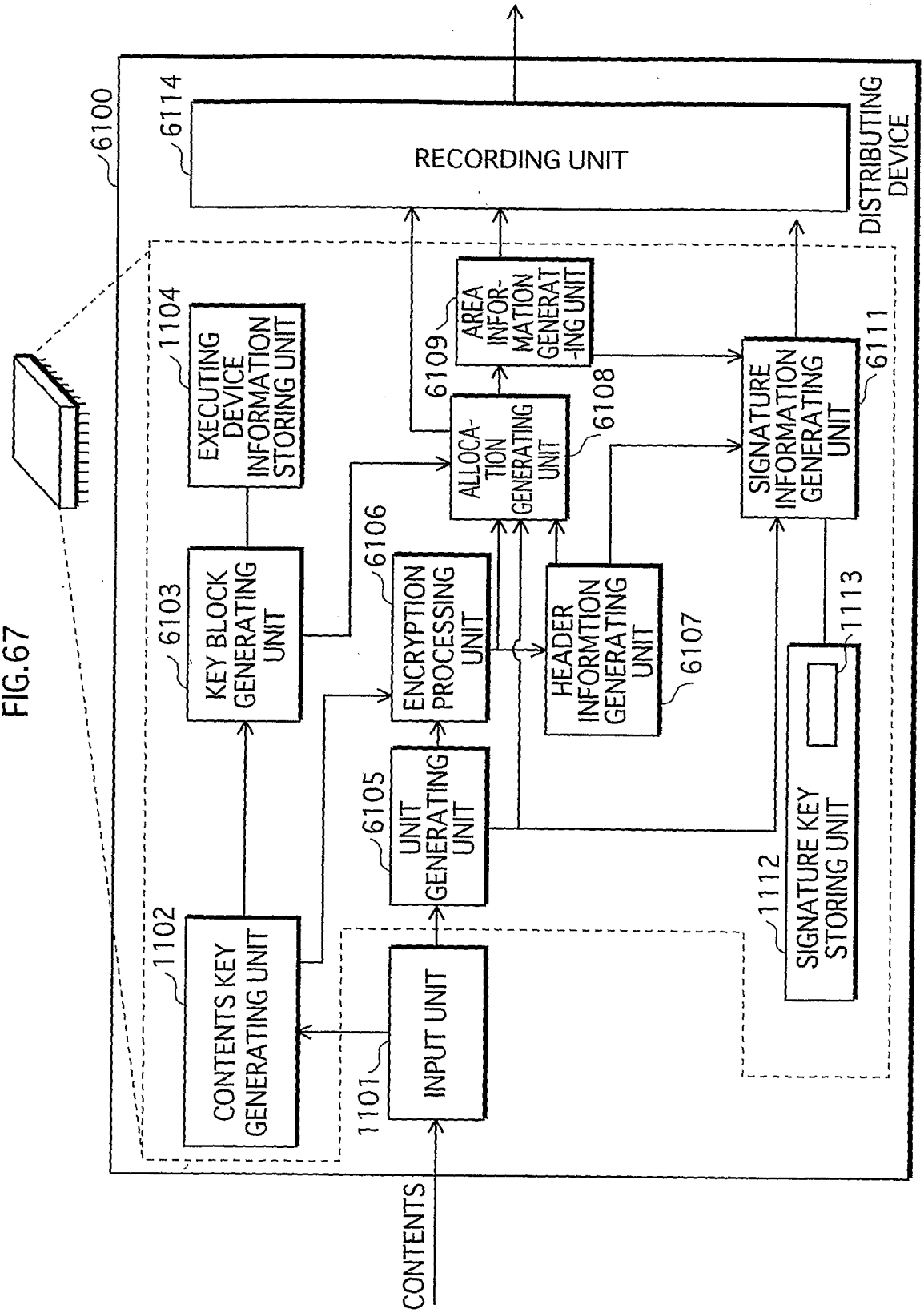

6100
DISTRIBUTING DEVICE
6114
RECORDING UNIT
1104
EXECUTING DEVICE INFORMATION STORING UNIT
6109
AREA INFOR-MATION GENERAT-ING UNIT
6108
ALLOCA-TION GENERATING UNIT
6111
SIGNATURE INFORMATION GENERATING UNIT
6106
ENCRYPTION PROCESSING UNIT
6103
KEY BLOCK GENERATING UNIT
6107
HEADER INFORMTION GENERATING UNIT
1113
6105
UNIT GENERATING UNIT
1112
SIGNATURE KEY STORING UNIT
1102
CONTENTS KEY GENERATING UNIT
1101
INPUT UNIT
CONTENTS

FIG.68

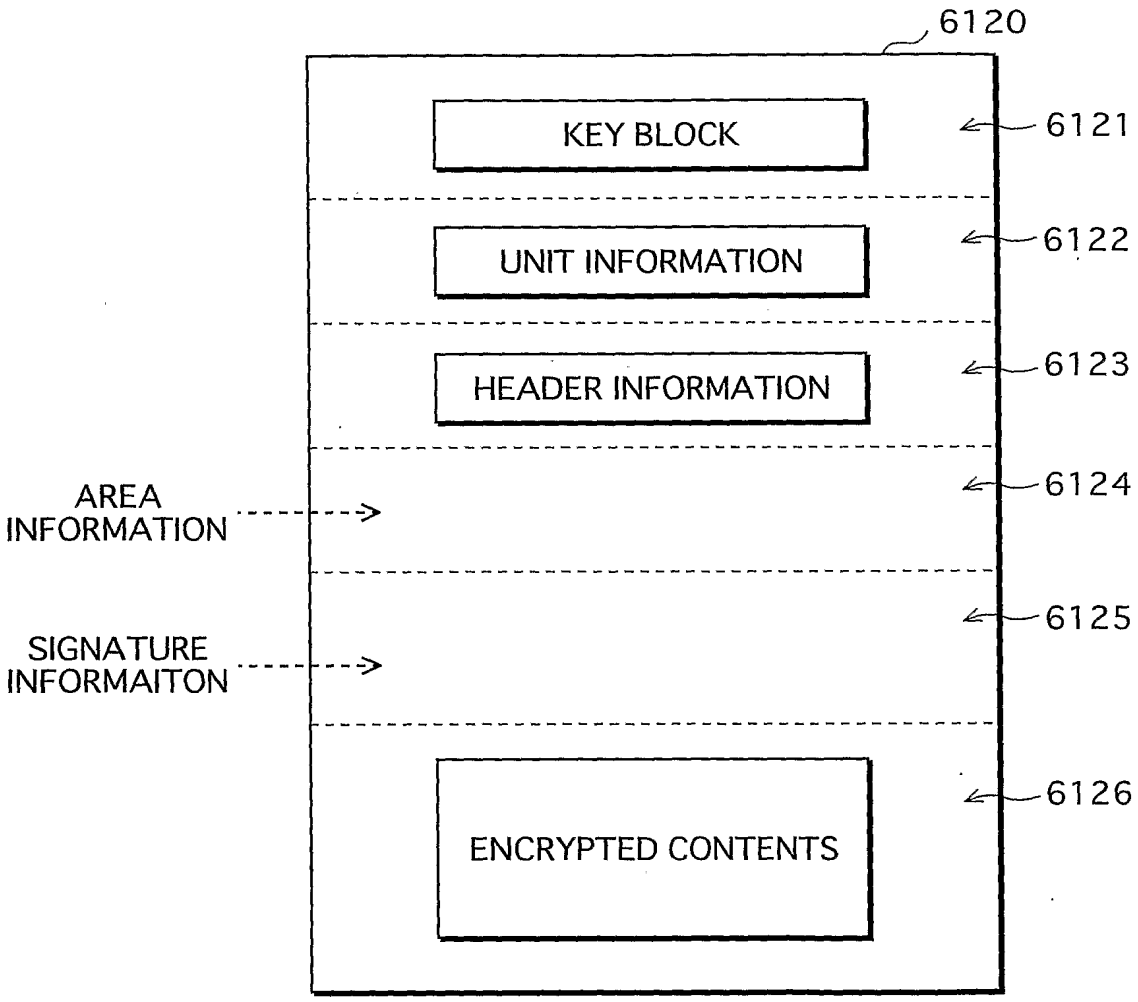

6120
KEY BLOCK
6121
UNIT INFORMATION
6122
HEADER INFORMATION
6123
6124
AREA INFORMATION
6125
SIGNATURE INFORMAITON
ENCRYPTED CONTENTS
6126

FIG.69

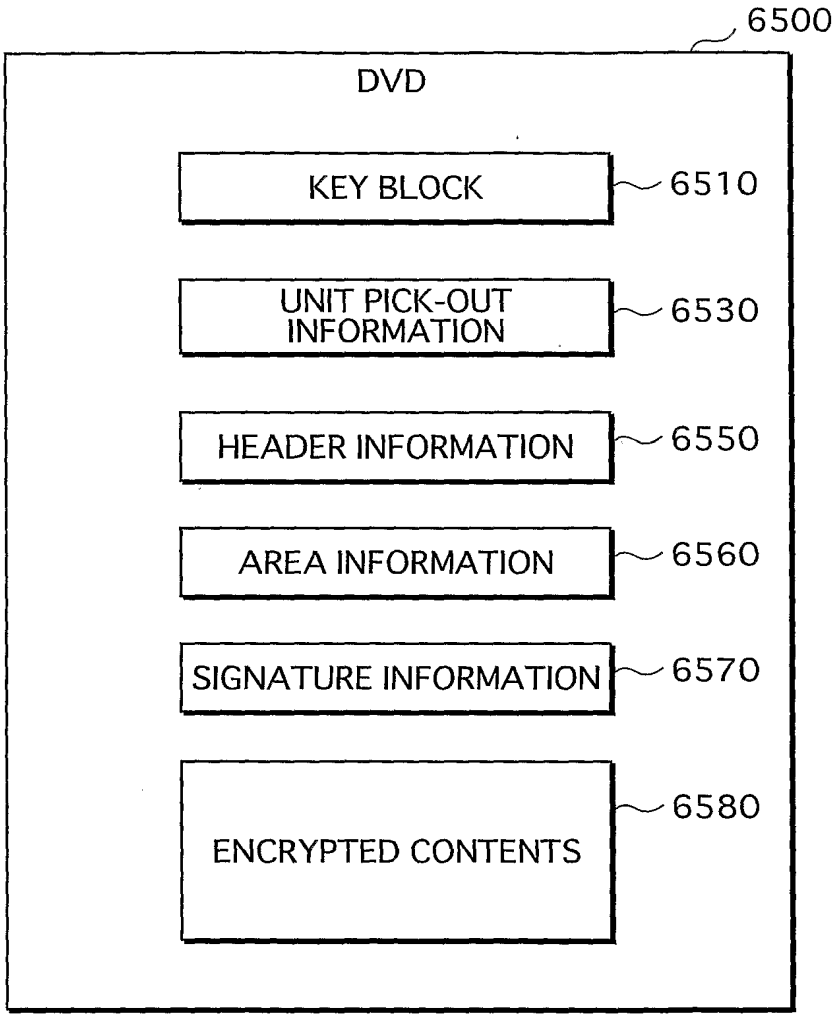
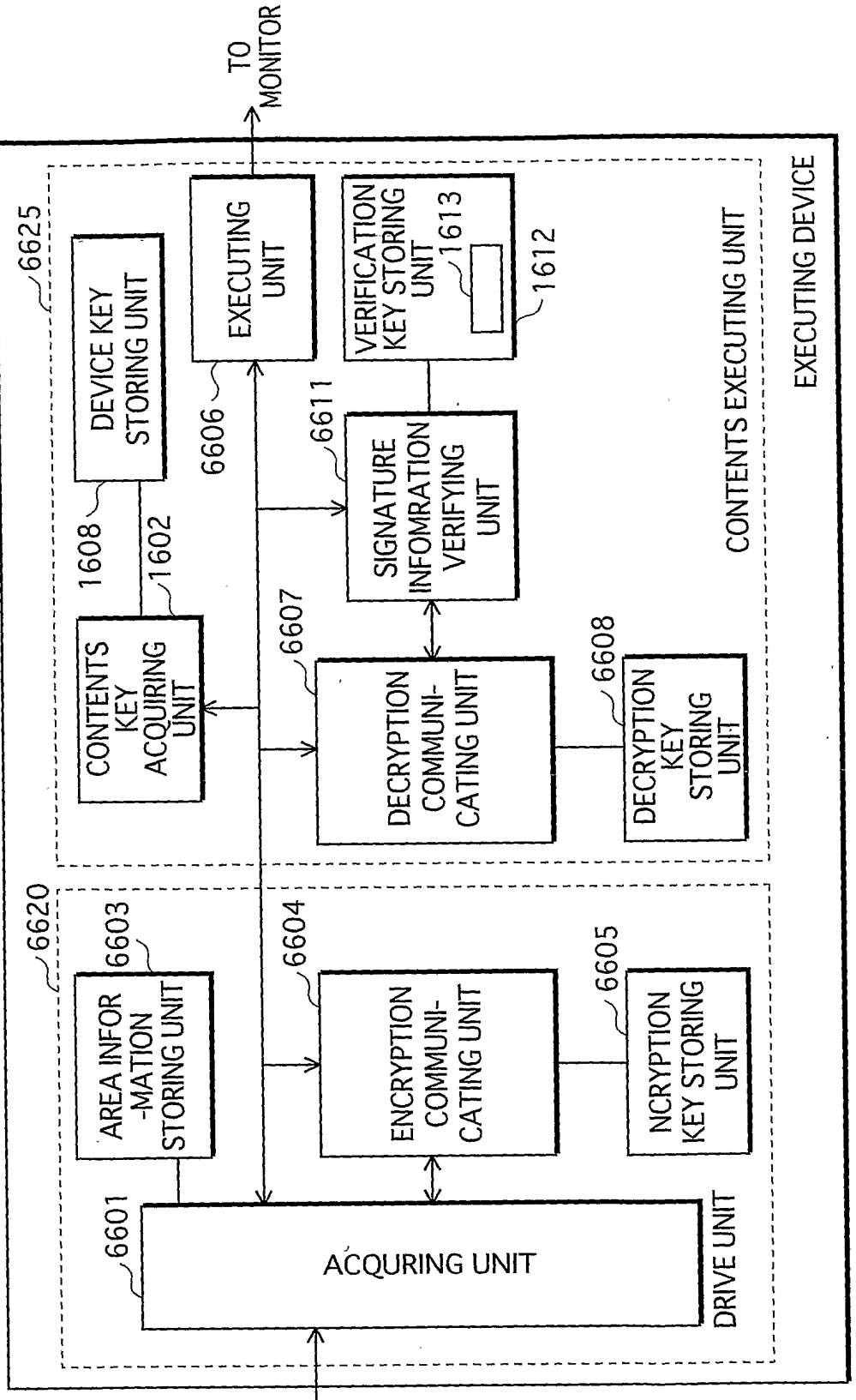
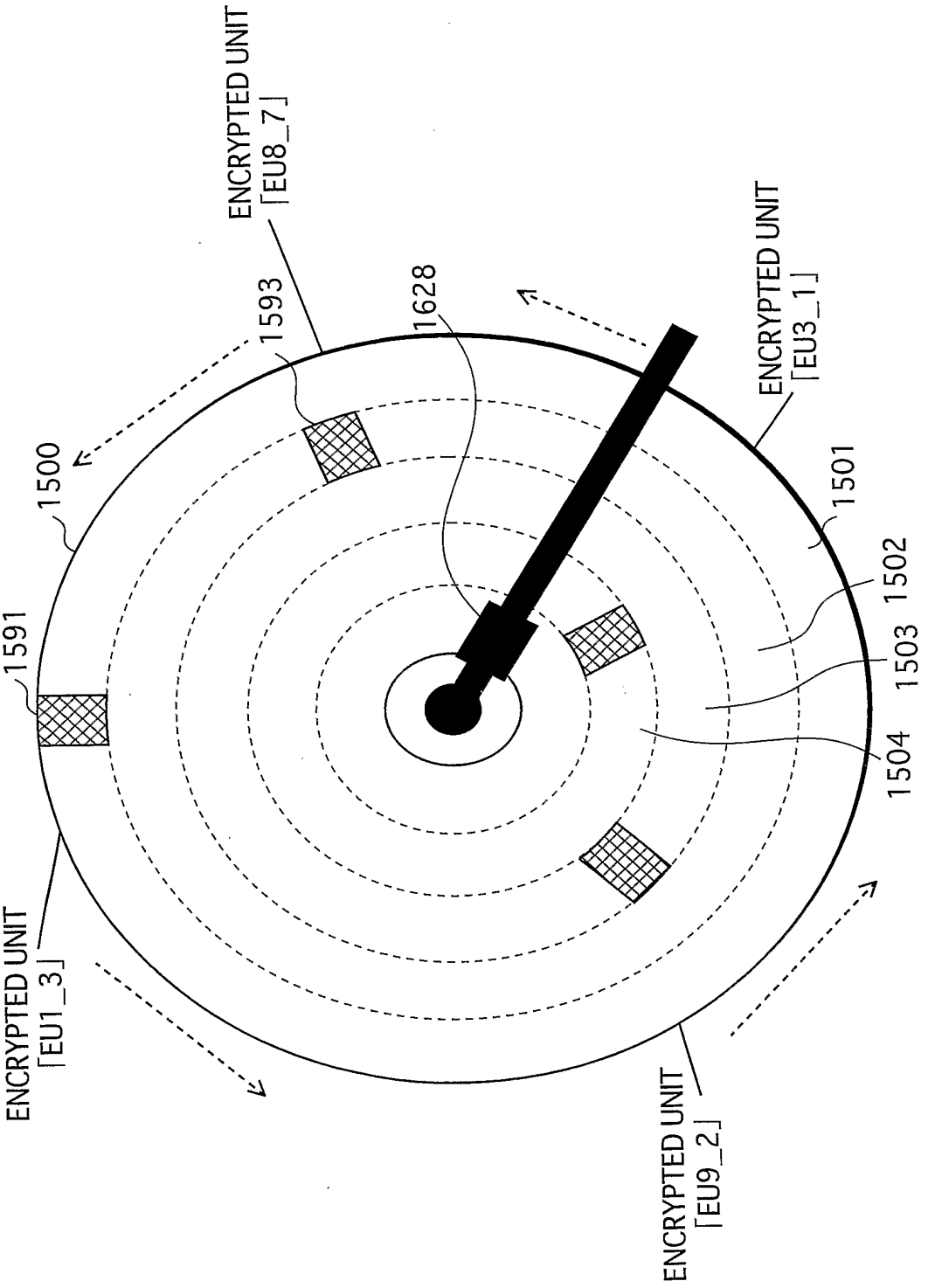

6500
DVD
KEY BLOCK
6510
UNIT PICK-OUT INFORMATION
6530
HEADER INFORMATION
6550
AREA INFORMATION
6560
SIGNATURE INFORMATION
6570
ENCRYPTED CONTENTS
6580

FIG.70




6605:ENCRYPTION KEY STORING UNIT
1612:VERIFICATION KEY STORING UNIT

FIG.71


ENCRYPTED UNIT
[EU8_7]
1593
1628
ENCRYPTED UNIT
[EU3_1]
1500
1501
1502
1503
1504
1591
ENCRYPTED UNIT
[EU1_3]
ENCRYPTED UNIT
[EU9_2]